CYNGOR SIR CEREDIGION
CEREDIGION COUNTY COUNCIL

REGULATION OF INVESTIGATORY

POWERS ACT 2000 PART II

Directed Surveillance, Use of Covert Human Intelligence Sources and Obtaining Communications Data

CORPORATE POLICY

AND

PROCEDURES DOCUMENT

- **Re-adopted by Council 29th June 2017**
- **Re-amended by SRO 5th October 2017**

INDEX

CEREDIGION COUNTY COUNCIL
COVERT SURVEILLANCE - POLICY STATEMENT

Introduction

1. Ceredigion County 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. Ceredigion County 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:

   - Human Rights Act 1998
   - Regulation of Investigatory Powers Act 2000
   - Protection of Freedoms Act 2012
   - Data Protection Act 1998

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.
- Covert surveillance [regulated by 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 by the Council's Cabinet, to ensure it remains fit for purpose.

11. The operation of the Council' RIPA activity shall be overseen and monitored by the Council's Overview and Scrutiny Coordinating 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 Monitoring Officer (Senior Responsible Officer).

Date ……..

CEREDIGION COUNTY COUNCIL

COVERT SURVEILLANCE - PROCEDURES DOCUMENT

PART 1 – INTRODUCTION

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 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.

As well as the Act 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) conducted by Council employees is carried out appropriately and on a lawful basis. This document should be read in conjunction with Home Office Codes of Practice on Covert Surveillance and Property Interference, Covert Human Intelligence Sources, Camera Code of Practice and the Office of Surveillance Commissioners Procedures and Guidance.

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 on the basis of 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 Part 7 – 'Dealing with complaints' of this document.

Scope of this document

This document explains:

- The Council's statutory responsibility to comply with RIPA when undertaking covert surveillance, using a covert human intelligence source (a CHIS) and accessing communications data;
- What "covert surveillance" and "covert human intelligence source" mean;
- What is meant by communications data and how it can be accessed;
- Issues which Council employees must consider under RIPA;
- The procedure Council employees need to follow when applying for RIPA authorisations.

The policy only applies 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. It does not apply to observations or surveillance which are not carried out covertly, e.g., use of overt CCTV cameras or unplanned observations made as an immediate response to events.
The Information Commissioner has issued a separate Code of practice on the use of CCTV surveillance.

Ceredigion County Council's statutory responsibility

The Council has a statutory responsibility to comply with the Human Rights Act 1998 and the European Convention for the Protection of Human Rights (ECHR).

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

Article 8 of the ECHR provides that:

- 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 is:
    a) in accordance with the law; and
    b) is 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) of the European Convention on Human Rights which is now enshrined in English law through the Human Rights Act 1998. This s 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 to be 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 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 2014 states that elected Members should review the Authority’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 local authority’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 2014, considers that councils should appoint a Senior Responsible Officer (SRO).

Ceredigion County Council’s Senior Responsible Officer (SRO) is the Monitoring Officer. The SRO should be able to advise staff 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;

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 Senior Responsible Officer will be responsible for overseeing and co-ordinating the:

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

2. annual review by Cabinet 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 Authority, including identifying individual and corporate training needs, and dissemination of information.

Authorising Officers (AO's)

RIPA requires that when the Council undertakes "covert directed surveillance", uses a "covert human intelligence source" (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 Authorising Officer (AO's) for a local authority can be a Director, Head of Service, Service Manager or equivalent.

Directorates may therefore currently nominate officers from at least Head of Service level, who can authorise these activities either as an "Authorising Officer" (AO's) for the purposes of directed covert surveillance or use of a CHIS, or as a "designated person" for the purposes of communications data.

Pursuant to the Council's new structure for future delivery of services, effective from 1st September 2015, and further to the Council's Resolution made on 22nd October 2015, the following officers will be authorised to act as AO's

- **Chief Executive**
- **Head of Lifestyle Services**
- **Head of Financial Services**
- **Head of Human Resources**

Limitation 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), which came into force on 1 November 2012 imposed further restrictions on local authorities' use of RIPA.

It restricts Authorising Officers 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 Authority 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 Authorising Officer is in any doubt about authorising any surveillance activity, they should seek advice from the SRO.

Note that RIPA does not enable a local authority to make any authorisations to carry out intrusive surveillance (for further details, refer to Part 2 of this document).

Urgent cases

The 2010 Order (No. 521) does not make provision for more junior officers to authorise in emergency circumstances.

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.

The power to make urgent oral authorisations has now been removed, because Section 43 (1) (a) of RIPA no longer applies to authorisations requiring a Magistrate’s approval.

All authorisations, even if urgent must therefore be made in writing.

The role of Justices of the Peace (MAGISTRATE)

Since 1st November 2012, the authorisation process for “covert directed surveillance”, use of a “covert human intelligence source” (CHIS) and requests for “communications data”, is subject to judicial approval and any authorisation granted by a local authority must be approved by a Justice of the Peace. See part 5 of this document for further information on seeking judicial approval.

The role of the Office of the Surveillance Commissioners (OSC)

The Office of Surveillance Commissioners acts as the regulatory body in respect of the Directed Surveillance and Covert Human Intelligence Source aspects of RIPA. It is this office that 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 OSC does not give legal advice, although guidance may be given, when appropriate to request originating from the Senior Responsible Officer of a public authority**.**

The role of the Information Commissioners Office (ICO)

The Information Commissioner's Office 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 – GUIDE TO SURVEILLANCE REGULATED BY CHAPTER 2 OF RIPA

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 European Convention of Human Rights (ECHR), particularly Article 8, the right to respect for private and family life.

The purpose of this document is to help officers decide what type of surveillance they are undertaking and whether it is regulated by Chapter 2 of RIPA.

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

- RIPA Statutory Codes of Practice

  - Covert Surveillance and Property Interference
    http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-covert

  - Covert Human Intelligence Sources
    http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-human-intel

  - Acquisition and Disclosure of Communications Data
    http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-acquisition

- SI 2010 N0.521 - Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010
  http://www.legislation.gov.uk/uksi/2010/9780111490365/contents

- 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/1500/contents

- Office of Surveillance Commissioner Procedures and Guidance (2014)
- Home Office Surveillance Camera Code of Practice (2013)

The techniques which local authorities may authorise

Part 2 of Chapter 2 of RIPA allows local authorities to authorise two of the three surveillance techniques it regulates.
The first issue for any local authority officer who is considering undertaking covert surveillance is:
is it something that can be authorised under RIPA?

The definitions of the different types of surveillance regulated by Part 2 of RIPA are as follows:

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

1. 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 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 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 in an immediate response to events?

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

Key Points to Note:

A. General observations do not constitute Directed Surveillance. The Covert Surveillance and Property Interference Code of Practice (Para 2.24) 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."

B. 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.

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

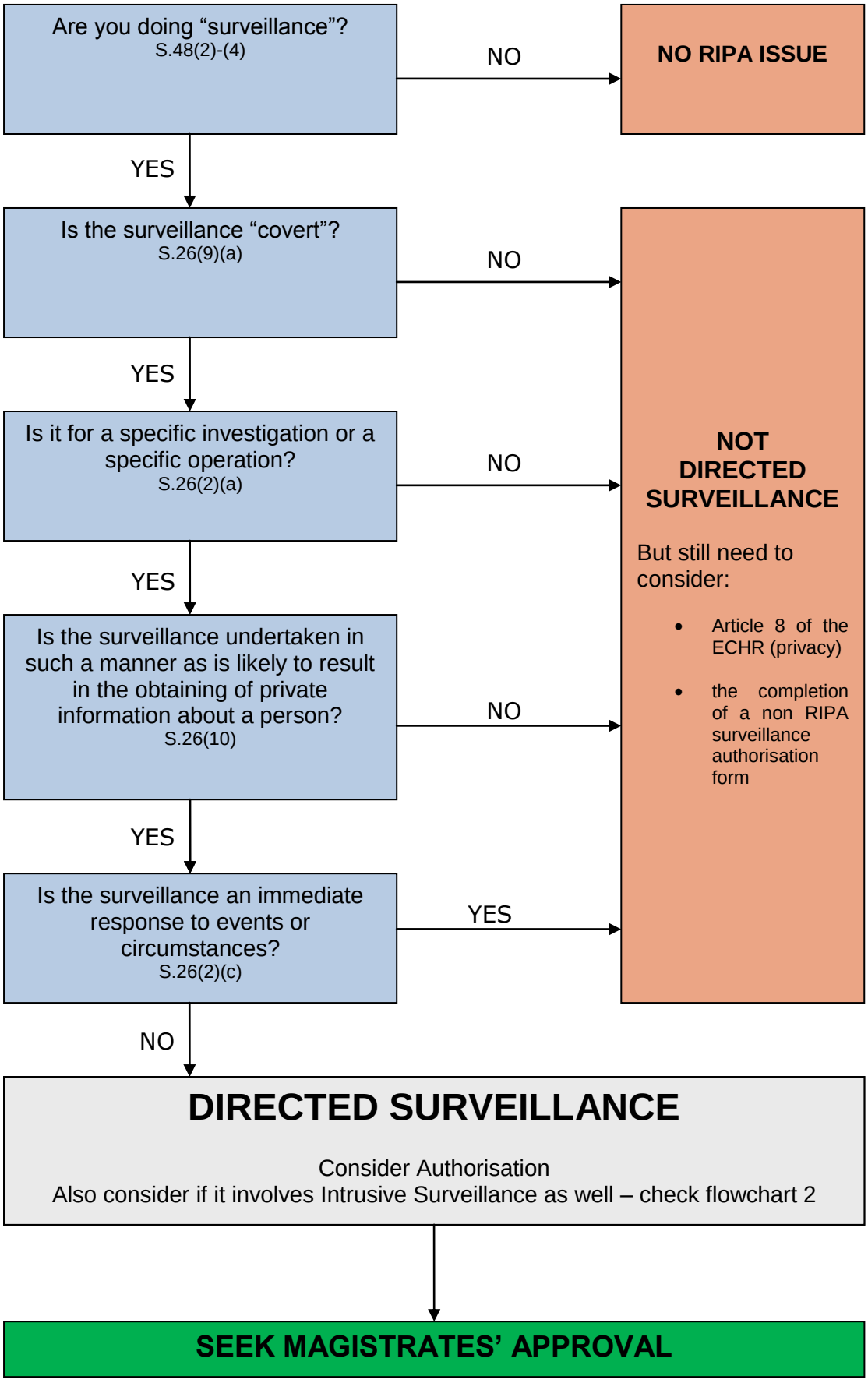
"2.4 The 2000 Act states that private information includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

2.5 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."

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, the surveillance can still be done but it will not require Directed Surveillance authorisation. The Covert Surveillance and Property Interference Revised Code of Practice (Para 2.23) 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."


Are you doing “surveillance”?
S.48(2)-(4)
NO
NO RIPA ISSUE
YES
Is the surveillance “covert”?
S.26(9)(a)
NO
YES
Is it for a specific investigation or a specific operation?
S.26(2)(a)
NO
NOT DIRECTED SURVEILLANCE
But still need to consider:
Article 8 of the ECHR (privacy)
the completion of a non RIPA surveillance authorisation form
YES
Is the surveillance undertaken in such a manner as is likely to result in the obtaining of private information about a person?
S.26(10)
NO
YES
Is the surveillance an immediate response to events or circumstances?
S.26(2)(c)
YES
NO
DIRECTED SURVEILLANCE
Consider Authorisation
Also consider if it involves Intrusive Surveillance as well – check flowchart 2
SEEK MAGISTRATES’ APPROVAL

2. <u>Intrusive Surveillance</u>: S.26(3) of 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 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?

*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):

"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.

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 chauffer-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.

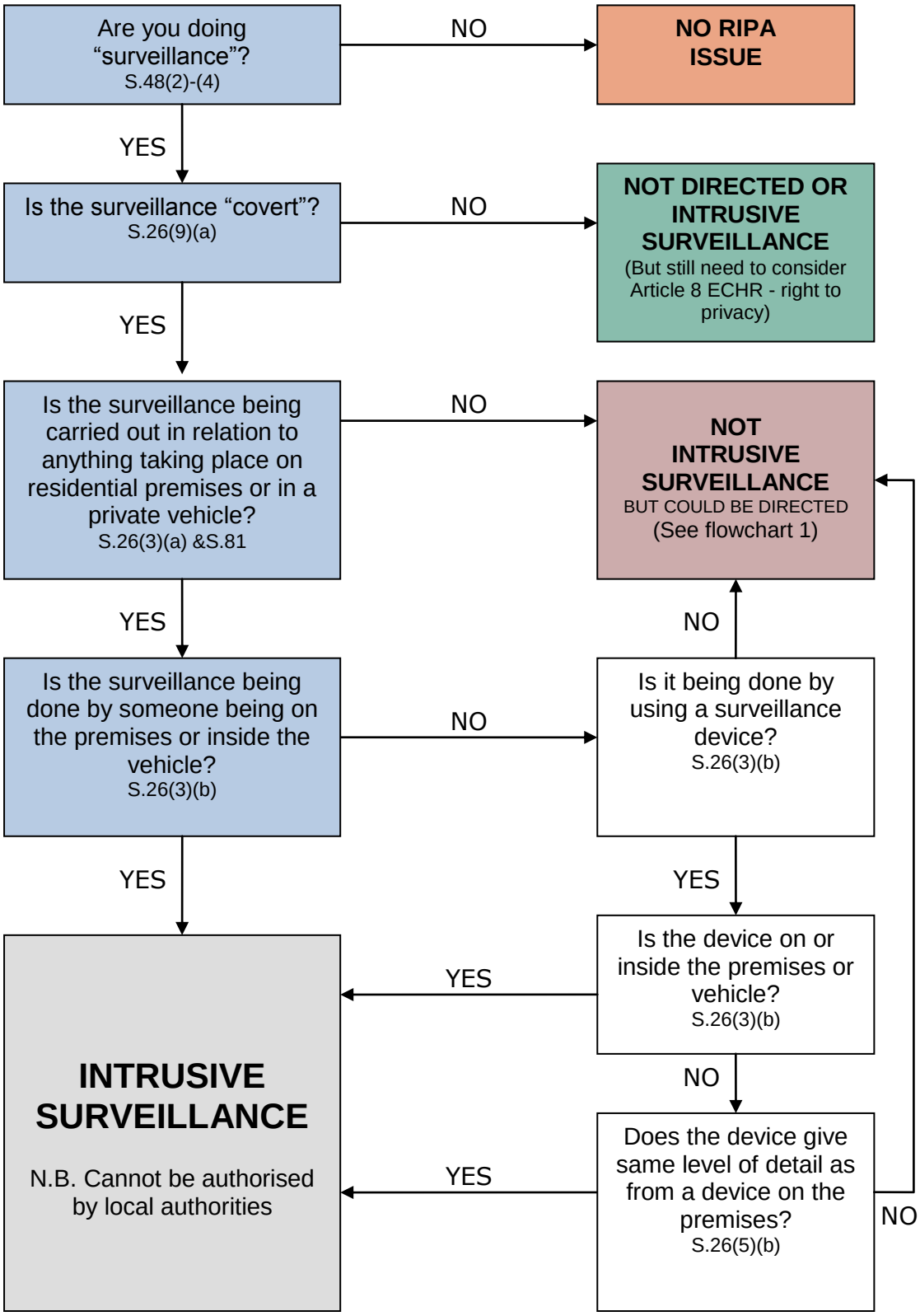
   However the words of S.26 (5) should be noted:

   "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?



3. Covert Human intelligence Source(CHIS)

This 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?
3. Is the covert purpose facilitating the doing of anything falling within paragraph (b) or (c) (above)?

*See **Flowchart 3** 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 Code of Practice (Para 2.14) 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."*
>
> **Care must be taken to ensure that someone who starts off 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 Home Office Covert Human Intelligence Sources Code of Practice (Para 2.12) states:

"The word "establishes" when applied to a relationship means "set up". It does not require, as "maintains" does, endurance over any particular period. Consequently, a relationship of seller and buyer may be deemed to exist between a shopkeeper and a customer even if only a single transaction takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the length of time of the contact between seller and buyer and the nature of any covert activity."

The Code of Practice also includes 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.

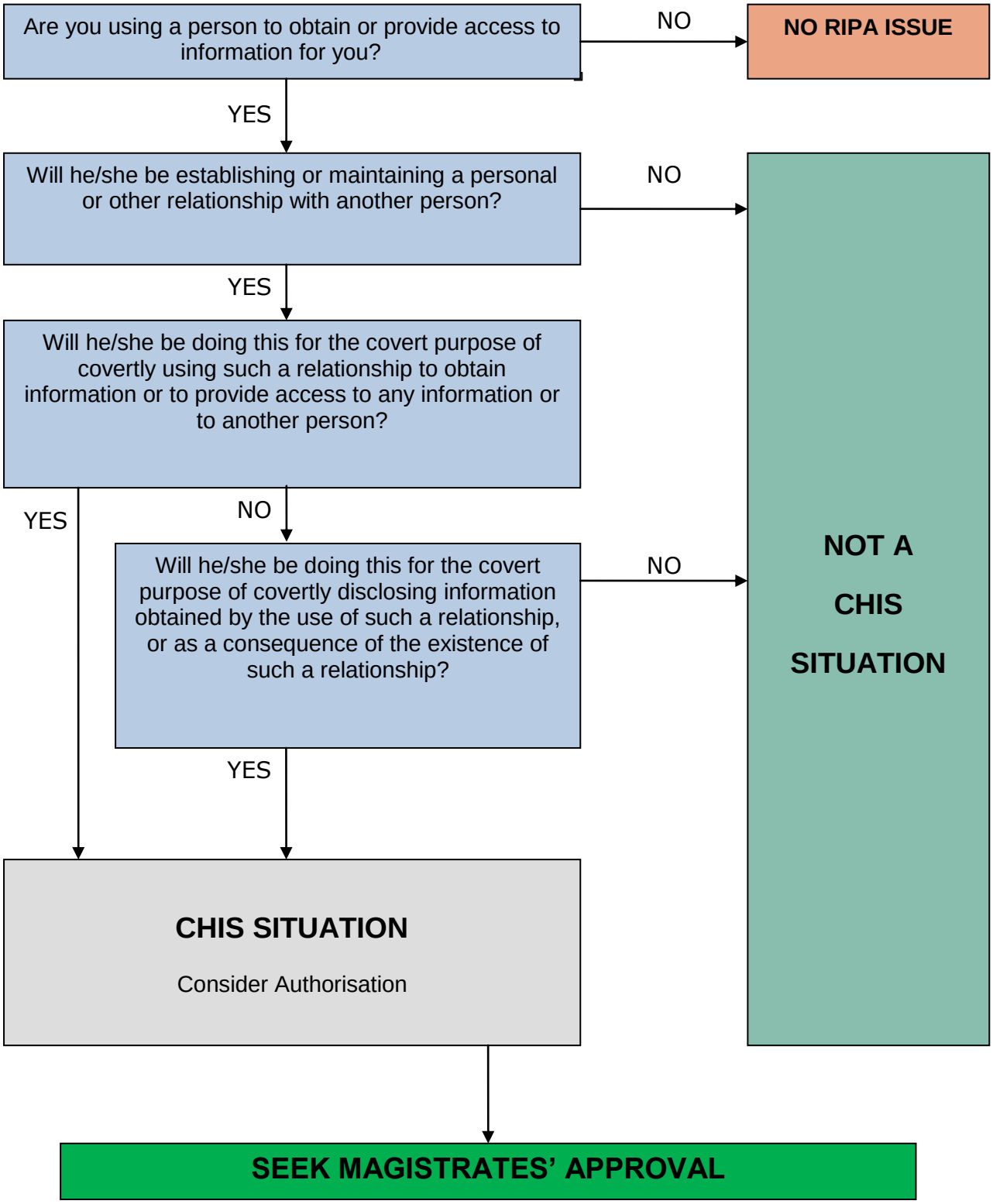
"Example 1: Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A juvenile is engaged and trained by a public authority and then deployed in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the 2000 Act that a public authority may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment but is not authorised as a CHIS, consideration should be given to granting a directed surveillance authorisation.

Example 2: In similar circumstances, intelligence suggests that a shopkeeper will sell alcohol to juveniles from a room at the back of the shop, providing he has first got to know and trust them. As a consequence the public authority decides to deploy its operative on a number of occasions, to befriend the shopkeeper and gain his trust, in order to purchase alcohol. In these circumstances a relationship has been established and maintained for a covert purpose and therefore a CHIS authorisation should be obtained."

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

- Better Regulation Delivery Office (BRDO) Code of Practice Age Restricted Products.

Flowchart 3 - Are you deploying a CHIS?



4. Communications Data

The RIPA (Communications Data) Order 2010 (SI 2010 no. 480) came into force on the 6th 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 to acquire information defined as "communications data". This includes subscriber data and service data but not "traffic data" as defined by the Act.

Definition 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.

"Communication data" is broadly split into 3 categories:

1. **S.21(4)(a) - "traffic data"**; This is usually data generated by the Communications Service Provider (CSP) in the process of delivering a communication. (***Not included in Local Authority authorisation***);

2. **S.21(4)(b) - Server use or billing information** - the use made of the service by any person i.e. ***itemised telephone records;*** e.g. numbers called, itemised connection records, itemised timing and duration of services, connection, disconnection and reconnection information; provision and use of forwarding/redirecting services; conference calls call messages call waiting & call baring information.

3. **S21(4)(c) - Postal records** including records of registered, recorded or special delivery postal items.

Examples:

- In the context of telephone data, it would include the telephone numbers of the phone from which the call was made and the number of the phone receiving the call. It also includes the date, time, duration and place of the call. It **DOES NOT** include the actual content of the telephone call.

- In respect of e-mail and the internet, it would include details of the subscriber account. It would also include dates and times when e-mails have been sent or received. The content of the e-mails are excluded from communications data. The websites are included but not the actual web pages that have been viewed.

- In the context of a letter, it would include the information on the envelope but not the contents of the letter. The information will therefore include the name and address of the recipient and the postmark showing when and where the letter was sent. It might also contain details of the address of the sender if recorded on the envelope.

Interception of Communications Data

The recording of telephone calls between two parties when neither party is aware of the recording **CANNOT BE UNDERTAKEN**, except under a warrant granted under Chapter I, Part 1 of RIPA. Such warrants are only granted by the Secretary of State and **such activity would NOT fall within the remit of local authority investigations.**

There may be situations where either the caller or receiver consents to the recording of the telephone conversation and, in such circumstances a Chapter 2 Part 1 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.

Employees

S.1 of RIPA does not apply to Local Authorities except where the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 - *SI2000/2699* applies. The legislative framework permits the Council without further authorisation to lawfully intercept its employees' e-mail or telephone communications and monitor their internet access for the purposes of prevention or detection of crime or the detection of unauthorised use of these systems. Further advice on these regulations should be sought from the SRO and/or the Head of Financial Services or the Head of ICT & Customer Services and regard should be had to the Council's internal Information Security Policy, and also the "ICO Quick Guide to the Employment Practice Code".

5. Non-RIPA Surveillance.

From time to time a local authority may wish to undertake covert surveillance, which is not regulated by RIPA. This is fine as RIPA is permissive legislation. More information is contained in a separate document "Non-RIPA Surveillance Guidance for Officers" (2016) (Appendix 5) outlining the procedures to be followed in respect of Non-RIPA Surveillance, including an application form.
Investigating officers are required to obtain a Unique Reference Number (URN) from the SRO prior to submission to the Authorising officer.

Authorising Officers include:
Deputy Chief Executive
Head of Financial services
Head of Lifeystyle Services

Similar mechanisms for activity which cannot be protected by the 2000 Act 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 an useful audit of decisions and actions.The process reflects that of directed surveillance, save for the Judicial approval.

The Monitoring Officer will retain a register of Non-RIPA authorisations, together with copies of application forms

Authorisation under RIPA affords a public authority a defence under S.27 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.

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

. . .

6 Internet and Social Networking Sites (SNS)

1. The fact that digital/electronic investigation is now routine or easy to conduct does not reduce the need for authorisation. Investigating and Authorised Officers must take care to understand how the SNS systems work. AO's must not assume that one service provider is necessarily the same as another, nor assume that the services provided are the same.

2. It is the responsibility of the individual to set adequate privacy settings to protect unsolicited access to private information. Data published, and therefore no longer under the control of the author, should not automatically be regarded as "open source" or publicly available. The author has a reasonable expectation of privacy if access controls are set. Some data may be deemed to be private communication still in transmission (eg instant messages).

3. Where privacy settings are available but not applied, the data may be considered to be open source – in such cases on authorisation is not usually required.

   Repeat viewing of open source sites may constitute directed surveillance on a use by case basis.

   The nature of the media is relevant.

   Example1,
   "Facebook" -if the data is communicated only to "Friends", it may reasonably be regarded as private information, with an expectation of privacy, as the information is only communicated to an exclusive group.

   Example 2
   "Twitter"-this may be regarded as communication to the world at large, although where search criteria are entered, it may become directed surveillance.

   If any member of the public can access the information (eg where there is no veto mechanism), it is not private information.

Open source information does not usually require authorisation. However, if a profile is built up of an individuals' lifestyle, it may become Directed Surveillance.

4. Assuming that there is no warrant authorising interception in place (pursuant to S48(4) RIPA), if is considered necessary and proportionate for a Local Authority to breach access controlled covertly, the minimum requirement will be a Directed Surveillance authorisation.

5. An authorisation for use and conduct of a CHIS is necessary if there is ongoing interaction, and a relationship is established or maintained by a member of a public authority, or by an agent acting on its behalf (ie the activity goes further than a mere reading of the content of the site).This could occur if an officer covertly asks to become a "friend" of someone on a SNS.

6. CHIS authorisation is only required when using an internet trading organisation, such as E-Bay or Amazon Marketplace, when a covert relationship is formed. The use of disguised purchase details in a simple overt electronic purchase does not require a CHIS authorisation, because no relationship is usually established at this stage. If a relationship is established or maintained by a member of a public authority or by a person on its behalf (ie. the activity is more than a mere reading of the sites content) a CHIS authorisation is necessary.

7. It is not unlawful for a member of a public authority to set up a fake identity. However, it is inadvisable for such an individual to do so for a covert purpose without authorisation.

8. 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 authorisation, nor without the consent of the person whose identity is used, and without due consideration being given to protection of that person. The consent must be explicit (in writing) as to what is, and is not to be done.
9. Using photographs of other person without their permission to support the false identity infringes other laws.

7. **CCTV**

The Council's CCTV system for town centres is an overt system. Members of the public will be aware that such systems are in use.

The operation of this system is covered by the Data Protection Act 1998, and the Home Office Surveillance Camera Code of Practice 2008 (as amended by the Home Office Surveillance Camera Code of Practice (2013).)

A separate document exists detailing the use of the system:

Operation of Public CCTV – Ceredigion County Council and Heddlu Dyfed-Powys Police (November 2010). This document was in the process of being reviewed, to take account of recent legislation and Guidance**,** and OSC Inspector recommendations

On 1st August 2014, the Council's overt town centre CCTV system was decommissioned.

This document will not now be reviewed.

See Part 4 below – Guidance for Authorising Officers.

Also ***Flowchart 4 –Authorising Non-RIPA Surveillance***

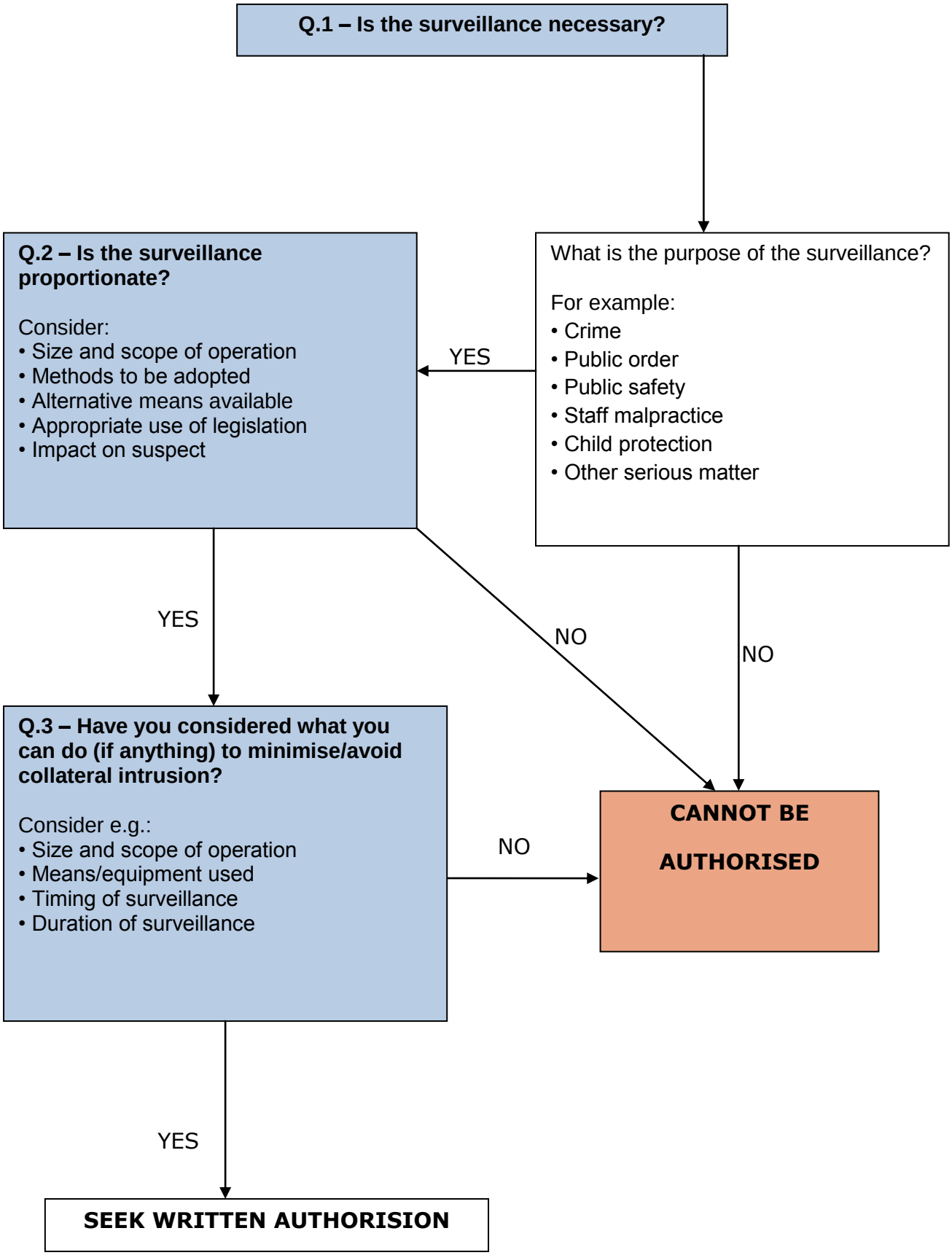
Data Protection Compliance

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.

Flowchart 4 - Authorising Non-RIPA Surveillance



PART 3 – PROCEDURES FOR OBTAINING AUTHORISATION

1) **Directed Surveillance Authorisation**

If you believe that your intended actions fall under the definition of directed covert surveillance, you will need to apply for a RIPA 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, he/she 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, Strategic Director or Head of Service.

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

Role of the Investigating Officer – Applicant

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

- 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
- 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

You will need to make an application on the relevant form which can be downloaded from the Home Office website, http://security.homeoffice.gov.uk/ripa

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
- 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.

Sample forms are annexed at **Appendix 1**, with detailed guidance on completion of relevant forms. **Flowchart 5** 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**
- **OSC Procedures & Guidance Document**
- **This policy**
- **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.

2) CHIS authorisation 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.

If any Council officer intends to use a CHIS, advice and guidance should be sought from Legal Services **before any steps are taken**.

NB 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 are satisfied.

Where the surveillance involves the deployment of juveniles or vulnerable people as a CHIS, then the authorisation must be sought from the Chief Executive or, in her absence, Head of Legal Services.

If any Council officer intends to use a juvenile CHIS, advice and guidance should be sought from Legal Services **before any steps are taken**.

Completing the Forms

You will need to make an application on the relevant form which can be downloaded from the Home Office website, http://security.homeoffice.gov.uk/ripa. 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
- Sequential Unique Reference Number (URN) obtained from the SRO and entered on to the form
- 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 policy
- OSC procedures And Guidance Document
- ACt NOW Toolkit

Sample forms are annexed at **Appendix 2**, with detailed guidance on completion of the relevant forms. **Flowchart 5** 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 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.
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
- That records are kept of all contacts and communications between the CHIS and the Council/ relevant officer at the Council.

3) Obtaining Communications Data Through NAFN's SPOC

Ceredigion County Council utilises the services of the National Antifraud Network (NAFN) to act as an accredited Single Point Of Contact (SPOC) with Communications Service Providers (CSP) and Internet Service Providers (ISP).

Since 2012 the procedure for seeking authorisation for accessing communications data is generally similar to that described for covert directed surveillance but with the additional involvement of NAFN as a SPOC.

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 application form online and it is then submitted electronically to one of the SPOCs at NAFN, who will advise the applicant of any need for changes. The relevant forms can also be downloaded from the Home Office website, and sample forms are attached at **Appendix 3.**

The NAFN officer appointed as SPOC, amongst other things, carries out a quality control role and advises the investigating officer and the Designated Person i.e. the Authorising Officer on various matters, e.g. whether the application meets the statutory requirements, whether the information being sought can be easily obtained by the Communications Service Providers (CSP) or Internet Service Providers (ISP) and whether the application would be cost effective. The NAFN SPOC will also be the contact officer for all liaisons with CSPs and ISPs.

Ceredigion County Council has two officers who currently undertake the role of "designated person" to authorise communications data requests:

- Head of Lifestyle Services, and
- Head of Financial Services

Designated Persons must have current working knowledge of human rights principles, specifically those of necessity and proportionality, and how they apply to the acquisition of communications data.

In addition, Ceredigion County Council has a Home Office accredited officer designated to undertake the role of SPOC. However, only in exceptional circumstances, such as the unavailability of the NAFN website would investigating officers be expected to complete paper forms and submit their forms to the Authority's own SPOC to complete the authorisation process. The officer designated as the Authority's SPOC is the:

- Consumer Services Manager (Trading Standards and Licensing).

Following the vetting process carried out by the SPOC, the Designated Person will then receive an e-mail (or the original forms when not using NAFN's electronic system), to say that there is an application form on the website for him/her to consider and the Designated Person completes the relevant part of the form to provide his/her decision.

Before the NAFN SPOC (or the Authority's SPOC) can use the authorisation to obtain the required communications data from the CSP, it cannot take effect until a Magistrate has approved it. The procedure for this is set out in part 5 of this document.

Following judicial approval, the NAFN SPOC (or the Authority's SPOC) then uses the authorisation process to obtain the required communications data from the CSP 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 CSP their SPOC will send a notice to the CSP in the usual way.

Using the NAFN website method has significant advantages over using the Authority's SPOC method as:

a) the turn round times for obtaining the communications data are considerably reduced,
b) the costs charged by the CSPs for providing the data are considerably less when using NAFN and
c) it ensures consistency across all Designated Persons and Local Authorities when acquiring communications data.

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

4) 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 CSP, so if it is discovered before this point it does not officially count as an error.

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 Interception of Communications Commissioner, 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 Authority 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;
- 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 Communications Service Provider;
- Notices being sent out to CSPs that were not produced by the Designated Person who authorised the application;

Where a telephone number has been sent to another Communications Service Provider 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 Designated Person will then decide whether it is necessary and proportionate for the excess data to be used in the investigation.

Any reportable error must be reported to the SRO and then to the Commissioner within 5 working days. The report must contain the unique reference number of the notice and details of the error, plus an explanation how the error occurred, indicating whether any unintended collateral intrusion has taken place and providing an indication of the steps that will take place to prevent a reoccurrence. The Reporting an Error by Accredited SPOC Form (CD5) should be used for this purpose.

If the report relates to an error made by a Communications Service Provider (CSP), the Authority must still report it, but should also inform the CSP to enable the CSP 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 Interception of Communications Commissioner's Office (IOCCO) inspectors and must be regularly reviewed by the SRO.

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
- 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
- The need for authorisation has to be judged at the time of the authorisation, not with the benefit of hindsight.

4) The lifecycle of an 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. See part 5 of this Policy and Procedural document for the procedure for seeking such approval.

Duration

Communications Data authorisations cease to have effect 1 month from the date of approval, Directed Surveillance authorisations 3 months from the date of approval, and CHIS authorisations 12 months from the date of approval. The duration of a juvenile CHIS authorisation is 1 month.

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. (Please consult the relevant Appendix attached and form for guidance on completing renewal forms).
See paragraphs 5.12-15 of the Home Office Code of Practice for Directed Surveillance and Property Inteference
Note: Renewals do not take effect until a Magistrate has approved the authorisation.

Reviews

When the authorisation is granted, the Authorising Officer 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 5.12-5.16 of Home Office Code of Practice for Directed Surveillance and Property Inteference

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 authorized in order that those conducting the surveillance are clear on what has been sanctioned at each stage in the authorization process.

An audit trail of the review criteria should be kept.

Cancellations

Authorisations will be cancelled when the Authorising Officer 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 Authorising Officer. 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).

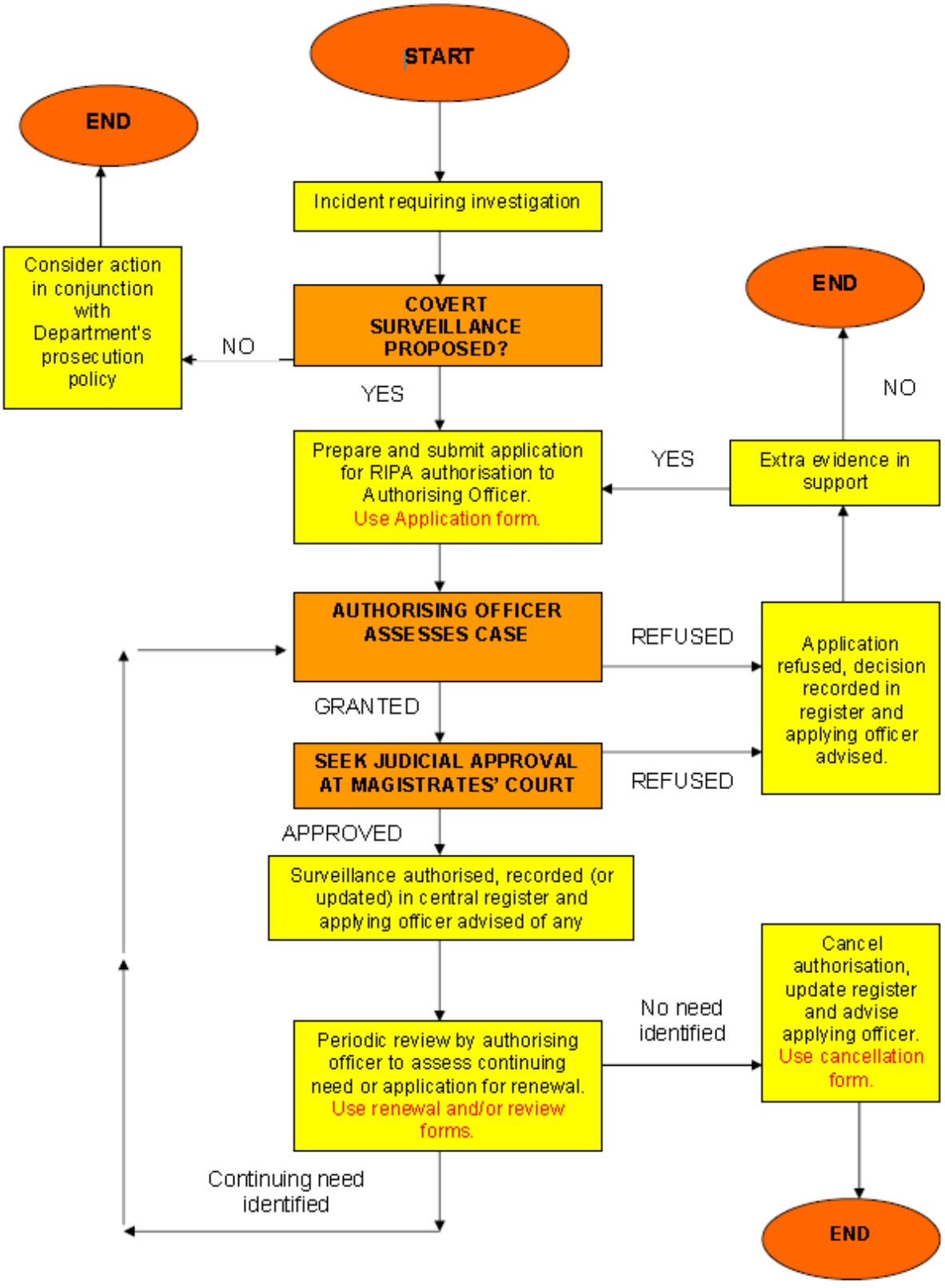
See pargraphs 5.17-18 of Home Office Code of Practice for Directed Surveillance and Property Interference.

Cancellations do not require judicial approval.

Central Register

All original authorisations should be kept on a Central Register maintained by the Monitoring Officer (acting as SRO) with the officer retaining a copy. Documentation of any instruction to cease surveillance must be retained. A record should be kept detailing the product obtained form the surveillance and whether objectives were achieved. Although the central register will be monitored by the SRO, it is ultimately the Authorising Officer's responsibility to ensure renewals and cancellations are up to date. The date of cancellation must be centrally recorded. The Central Register should also include details of any Magistrates approval.

Flowchart 5 – Basic Lifecycle of a Directed Surveillance Authorisation (similar lifecycle for a CHIS and/or Comms Data)



PART 4 – GUIDANCE FOR AUTHORISING OFFICERS

1) AUTHORISING DIRECTED SURVEILLANCE: 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.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 **must** be sought from the Head of Paid Service i.e. the Chief Executive or, in his/her absence, the acting Head of Paid Service.

If there is any doubt regarding sufficiency of rank you should contact the SRO (Monitoring Officer) for advice.

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 Consideration

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 6** 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.

Local authority Authorising Officers 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
- 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.
- 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 recognized 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. AO's must ensure that legal requirements are addressed throughout the life of an authorisation.

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

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 authorize 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 (Para 3.6) 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;
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 his own words why he believes the (RIPA) activity is necessary and proportionate. A bare assertion is not sufficient.

C. Can Collateral Intrusion be avoided or minimised?

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.

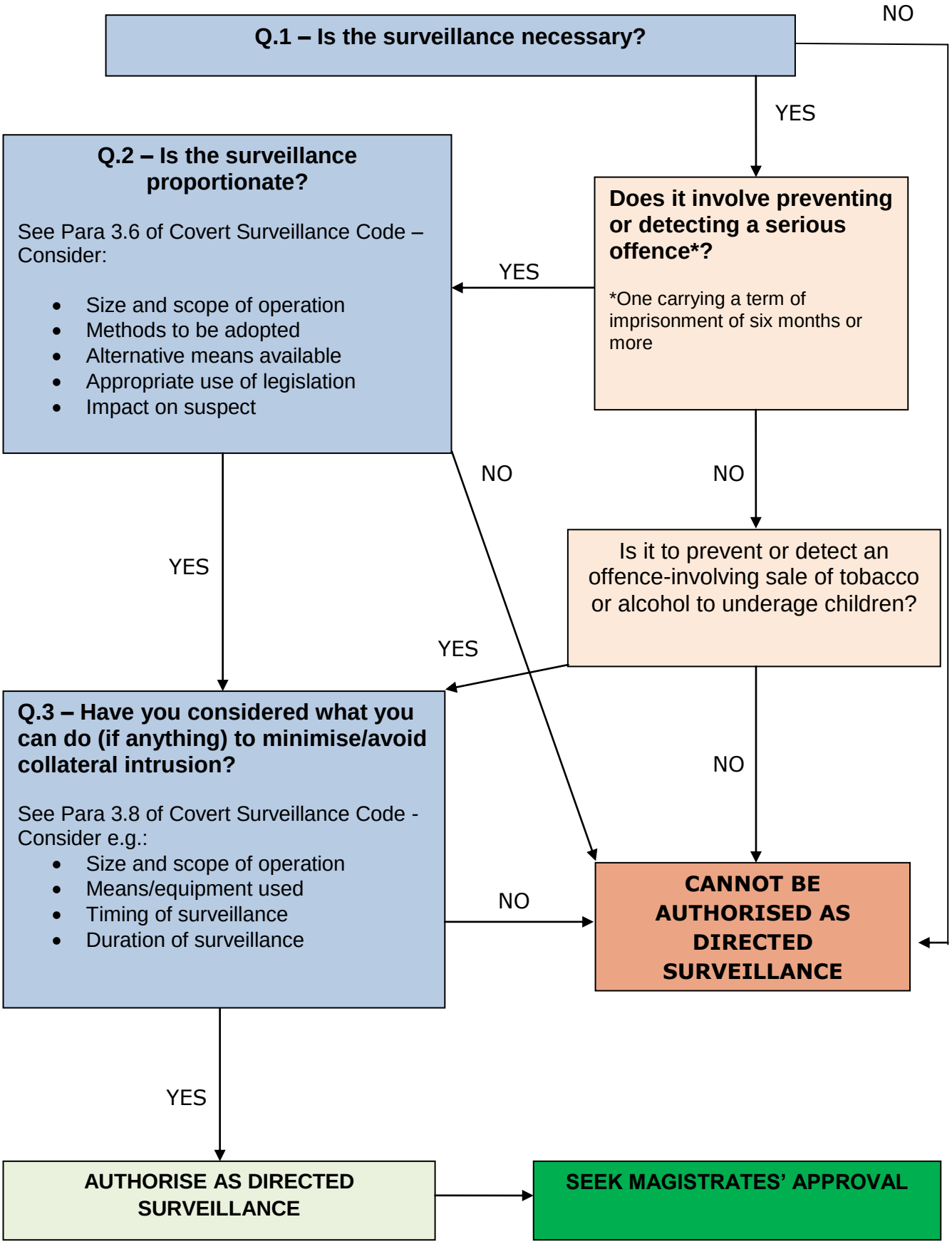
Investigating and Authorising Officers will need to ask themselves:

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 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

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 Magistrates' approval. See Part 5 for a detailed explanation of the procedure.

Flowchart 6 - Authorising Directed Surveillance



2) 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 authorize a 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 **must** be sought from the Head of Paid Service or, in his/her absence, the acting Head of Paid Service.

If there is any doubt regarding sufficiency of rank you should contact the Head of Legal Services for advice.

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).

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 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. 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 3.5) 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;
- 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.
- Proper and secure records to 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;

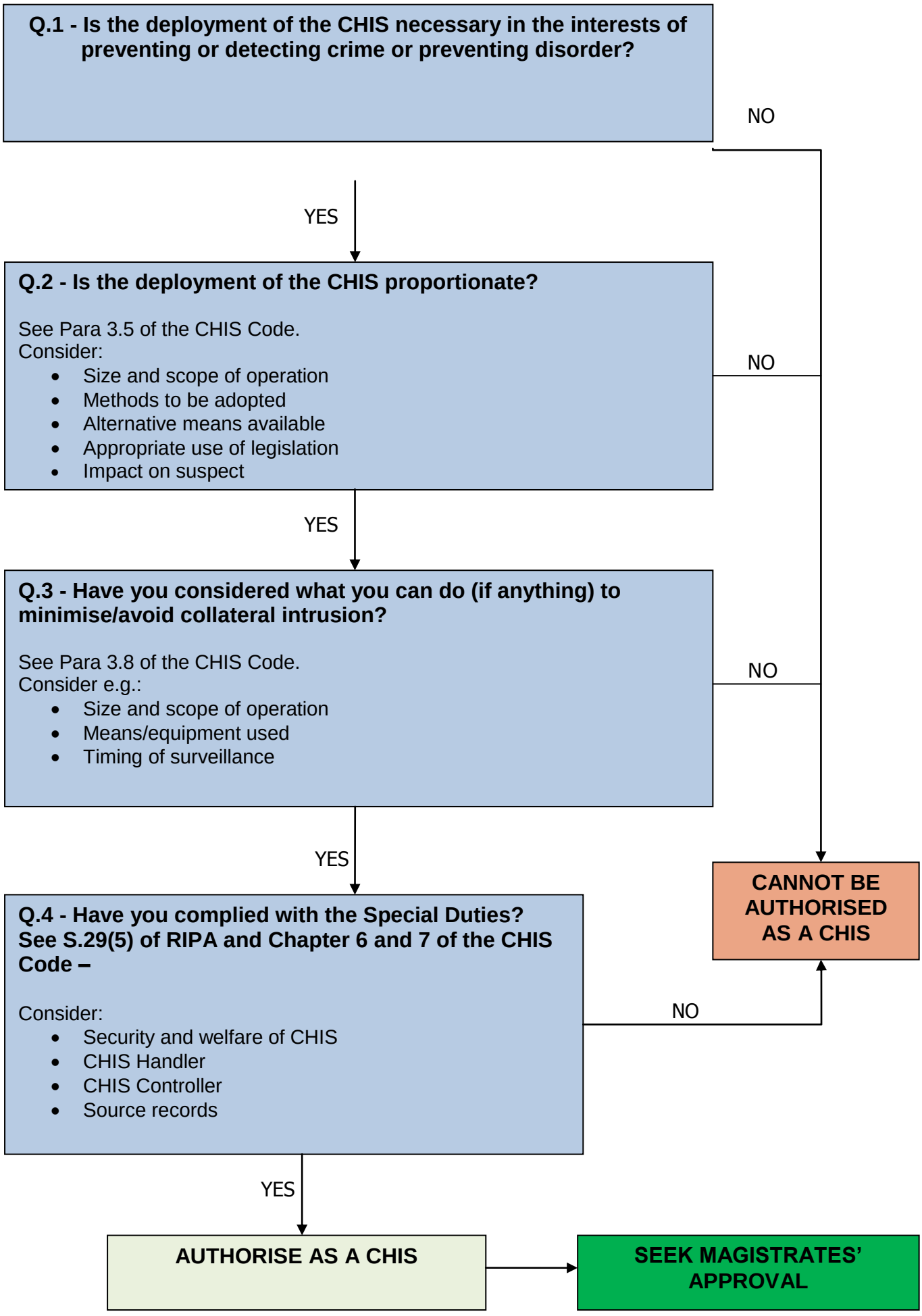
- the nature and magnitude of any risk of psychological distress to the CHIS arising in the course of, or as a result of, carrying out the conduct described in the authorisation has been identified and evaluated;

- 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;

- 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.

Next Stage: Once the use of a CHIS has been authorised, the next stage is to seek Magistrates' approval. See Part 5 for a detailed explanation of the procedure.

Flowchart 7 - Authorising a CHIS



3) AUTHORISING THE ACQUISITION OF COMMUNICATIONS DATA

Section 21 of RIPA provides a defence if acquisition and disclosure of communications data is challenged:

"(2) Conduct to which this Chapter applies shall be lawful for all purposes if -

(a) it is conduct in which any person is authorised or required to engage by an authorisation or notice granted or given under this Chapter; and

(b) the conduct is in accordance with, or in pursuance of, the authorisation or requirement."

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 Designated Person 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),

   - 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: http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa/forms/code-of-practice-acquisition

The Designated Person

After the SPOC has submitted the Application for Communications Data Form, along with the relevant draft notice(s) or authorisation(s), to a Designated Person, it is the Designated Person that will make the decision about whether or not the application will be approved.

The Designated Person will consider the form and then complete the Designated Person's part of the Application Form to state whether they grant or refuse the application. On the form the Designated Person must record:

- Why he/she believes acquiring the communications data is necessary;
- Why he/she believes the conduct involved in acquiring the communications data is proportionate;
- If accessing the communications data involves a meaningful degree of collateral intrusion, why he/she believes that the request is still proportionate;

Time Limits

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

The Designated Person shall endorse the draft notice or authorisation with the date, and if appropriate the time, at which he/she gives the notice or authorisation. This is the point at which the Designated Person approves the application.

If the Designated Person requires any advice they are able to obtain it from the NAFN SPOC (if using the NAFN secure website system), or the Authority's own SPOC in other cases.

All notices and authorisations requesting communications data from the service provider will only be valid for one month from the date on which the authorisation is granted or notice given.

Notices and authorisations can be renewed for a period of up to one month by the grant of a further authorisation or the giving of a further notice. A renewed authorisation or notice takes effect upon the expiry of the authorisation or notice it is renewing.

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

Note: The notices and authorisations does not take effect until a Magistrate has approved the authorisation. See part 5 of this Policy and Procedural document for the procedure for seeking such approval.

In the event of the cancellation of a notice, the SPOC must inform the relevant postal or telecommunications operator of the cancellation without delay.

Similarly, where the Designated Person considers that an authorisation should cease to have effect, because the conduct authorised becomes unnecessary or no longer proportionate to what was sought to be achieved, the authorisation should be withdrawn.

Designated Person's Consideration

Home Office Guidance on considerations of the Designated Person

The Designated Person must be able to show he/she has understood the need for the application and considered necessity and proportionality to a standard that will withstand scrutiny.

The Designated Person should tailor their comments to a specific application as this best demonstrates the application has been properly considered

If the Designated Person having read the application considers the Applicant has met all the requirements then he/she should simply record that fact. In such cases a simple note by the Designated Person should be recorded.

If the Designated Person 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.

Similarily, 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 Designated Person, the SPOC will retain the form and inform the applicant in writing of the reasons for its rejection. In the paper based system this is done using form CD2, but the NAFN SPOC will do so via the website.

If the Designated Person is recording their considerations within the NAFN database and is attributable to the Designated Person, a signature is not required.

PART 5 – SEEKING MAGISTRATES' APPROVAL

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 local authority surveillance under the Regulation for Investigatory Powers Act 2000 (RIPA).

Since 1st November 2012 local authorities are required to obtain the approval of a Magistrate 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 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 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.

See Flowchart 8 for summary of the Magistrates approval process

The 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 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 fulfill this role but the Authorising Officer 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) *(see Appendix 4 for an example with notes to assist completion).*

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 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. She/he 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 local authority 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 local authority 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 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 Magistrate 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 Magistrate 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.

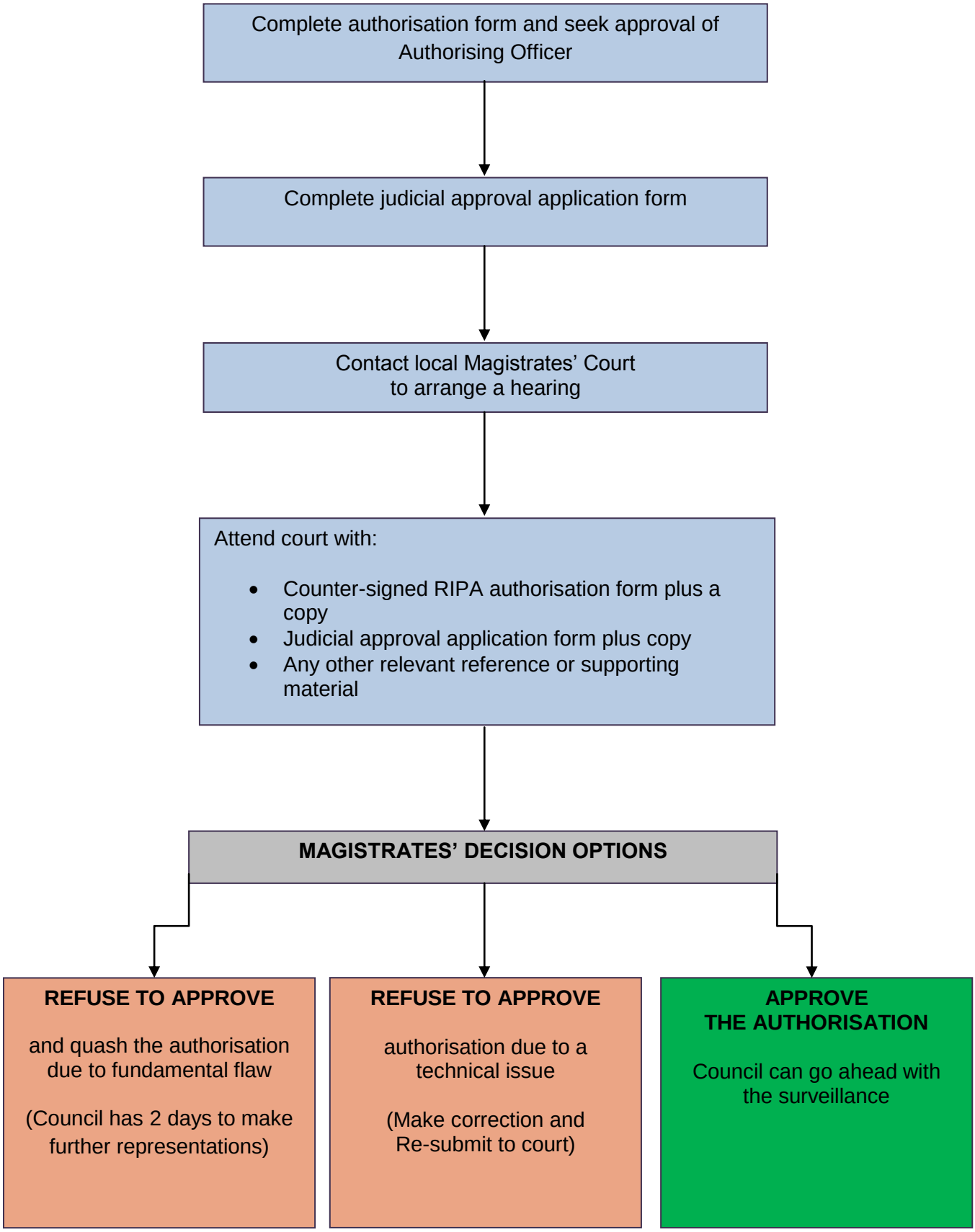
Appeals

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 a local authority 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.

Flowchart 8 - The Magistrates' Approval Process



PART 6 – THE CENTRAL REGISTER OF AUTHORISATIONS

A central register record of the following information relating to all authorisations will be held centrally by Legal Services and will be kept for at least 3 years from the ending of each authorisation and should be made available to the relevant Commissioner or an Inspector from the Office of Surveillance Commissioners upon request.

It will be the responsibility of the SRO or nominated representative to ensure that the register is maintained, overseen and documents securely filed/stored.

The records should contain the following information:

- Original authorisations (not copies)
- the type of authorisation;
- the date the authorisation was given;
- 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;
- 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

N.B. All investigating officer's should keep a copy of the authorisation within their own department and submit the original documents to the SRO. However, it is each Department's responsibility to securely retain all authorisations within their Departments and once an investigation is closed (bearing in mind cases may be closed sometime after the initial work) the duplicate records held by the Department should be disposed of in an appropriate manner i.e. treated as confidential waste and shredded

A Central record must be kept in respect of the use of CHIS as an official record of the current status.

However, in the case of authorisations in respect of communications data, the 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.

When the NAFN system is being used copies of the notices and authorisations are not routinely provided to the Designated but print-offs of the completed online application forms will be provided to the Applicant prior to seeking Judicial Approval.

Inspectors from the ICO will be able to obtain copies of all of these documents from NAFN.

The Monitoring Officer (acting as SRO) will have access to all of these forms as and when required.

The Central record should also contain a record of:

- Number of applications rejected by Designated Persons;
- 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);
- Number of times an urgent notice is given orally

The Authority's SPOC will keep a record of all applications, plus any notices and authorisations issued by the Authority. These records will include any errors that have occurred.

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 Authority's SPOC will request such information from NAFN on a quarterly basis.

PART 7 – DEALING WITH COMPLAINTS FROM THE PUBLIC

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 Complaints Procedure. 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. Complaints should be made in writing to:

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

APPENDIX 1
Forms for directed surveillance *(with notes to assist completion)*

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000
Application for Authorisation of Directed Surveillance

Sample Form with Notes to Assist Completion

This form is to be completed by an officer of the local authority seeking authorisation to carry out Directed Surveillance. Before completing it, you must satisfy yourself that you are doing Directed Surveillance as defined by RIPA. Please read chapter 2 of the Covert Surveillance Code of Practice.

Once completed, this form should be forwarded to the Authorising Officer for approval and to complete box 12 onwards. The next step is to seek the approval of a Magistrate. If this is granted, the authorisation will last for three months.

Code of Practice/Code: This is the RIPA Covert Surveillance Code of Practice.

Unique Reference Number (URN): This is a reference unique to each individual form but which also allows the form to be matched with other forms in the same investigation or which are issued by the same department. Some organisations devise a URN which comprises of the year, department initials, applicant initials and investigation number. In some cases the investigating department allocates the URN whilst in others this is done by the RIPA Co ordinator. There are no hard and fast rules.

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

This section is fairly explanatory. Where a third party (e.g. private detective agency or the police) is used to carry out Directed Surveillance on behalf of the authority or to give operational support, details of that party and their involvement should be recorded on this form. See paragraph 3.15 - 3.21 of the Code.

Unique Reference Number	

DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010; No.521. [1]

Insert the name and position of the Authorising Officer. This is the person who will decide whether or not Directed Surveillance should be authorised and will countersign this form. He/she must hold a rank in accordance with the above Order (i.e. Director, Head of Service, Service Manager or equivalent). Care should be taken to avoid more junior officers authorising surveillance. Each department, which makes regular use of Directed Surveillance, will have officers appointed as such. If in doubt consult the RIPA Co-ordinator.

2. Describe the purpose of the specific operation or investigation.

Explain the crime, which is being investigated. For example;

- "To investigate and gather evidence of a possible benefit fraud by the target."
- "To investigate instances of illegal dumping of waste at ...."
- "To investigate criminal damage which has been perpetrated against..."

If possible, include the relevant legislation that may be used to prosecute offenders and/or which gives you the power/duty to investigate the matter.

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, and recorder) that may be used.

Read the above carefully. Note the phrase "in detail." Therefore a response which merely states "Video camera and recording equipment will be installed at a fixed point" will not be adequate.

Your statement here needs to include what is going to be done, who is going to do it, when they are going to do it, where they are going to do it and how they are going to do it. Other points to address here include:

- How long will the surveillance last?
- Specific details about dates and times i.e. is it 24/7, at specific times of the day or at random times?
- Which premises are to be used and/or targeted?
- Which vehicles are to be used? Are they public or private?
- What type of equipment is to be used? e.g. covert cameras, audio devices
- What is the capability of the equipment to be used? e.g. zoom lense, remote controlled etc.
- Who else will be involved in the operation and what will be their role? e.g. private detectives, police

It may be appropriate to attach plans/maps showing where and how the surveillance will be conducted and indicating where any surveillance equipment will be installed.

Note that, if the Authorising Officer approves this surveillance, the authorisation will only cover you to do what you have stated here (subject to any amendments made by the Authorising Officer in box 12). Consequently you can only rely on section 27 ("the RIPA Shield/Defence") in so far as you were undertaking the activities set out in this section. Therefore it pays to include lots of detail.

[1] For local authorities: The exact position of the authorising officer should be given. For example, Head of Trading Standards.

Unique Reference Number	

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

Include as much information as you have. If you do not know the identity of the target then say so. You could include a general description of the target(s) e.g. "visitors and/or residents of ASBO lane (identities unknown) who are alleged to be selling counterfeit goods at the property."

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

Your statement here should be more detailed than in Box 2. You should give details of the precise information sought by doing the surveillance. For example:

- "To ascertain what time the suspect enters and leaves the building."
- "To capture images of the perpetrators of criminal damage at [place/address]."
- "To find out who is delivering the counterfeit goods to the suspect's premises [place/address]."
- "To corroborate the evidence of witnesses who have complained about racially aggravated anti social behaviour."

You may include a number of separate pieces of information it is hoped to be obtained by doing the surveillance e.g. "where the alleged perpetrator is dumping the illegal waste, who he is employing him and when it is being done."

6. Identify on which grounds the directed surveillance is <u>necessary</u> under Section 28(3) of RIPA. Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (SI 2010 No.521)

- ~~In the interests of national security;~~
- For the purpose of preventing or detecting crime
- ~~In the interests of the economic well-being of the United Kingdom;~~
- ~~In the interests of public safety;~~
- ~~for the purpose of protecting public health;~~
- ~~for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;~~

From 1st November 2012, local authorities can only authorise Directed Surveillance on the one ground: where it is necessary to prevent or detect crime. If you are not investigating a criminal offence (e.g. merely seeking to prevent disorder/anti social behaviour) then you cannot seek authorisation for this Directed Surveillance. Box 7 explains the requirements in more detail.

Unique Reference Number	

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 3.3]

The OSC Document states that the Authorising Officer must be satisfied that there is a necessity to use covert surveillance in the proposed operation. In order to be satisfied, there must be an identifiable offence to prevent or detect before an authorisation can be granted on the grounds falling within S. 28(3)(b) of RIPA.

From 1st November 2012, pursuant to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012, (SI 2012/1500), 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 (SI 2010 no.521). 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 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.

To address the above, you should explain here:

- The criminal offence you are investigating
- How it satisfies the six month threshold test (or falls within the exceptions) explained above
- How doing the Directed Surveillance will help the prevention or detection of the crime
- Any other evidence you have to link the target with the offender/offence which requires corroboration through surveillance

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.]
Describe precautions you will take to minimise collateral intrusion

When doing Directed Surveillance you may be invading the privacy of those who are not your target. RIPA requires you to think about their rights and what you can do to minimise the impact on them of your surveillance. People who may be the subject of collateral intrusion include:

- customers or workers at business premises
- visitors to a property
- friends or relatives of the suspect
- other people living on a housing estate where covert cameras have been set up to capture vandalism

The Code of Practice states:

"3.9 ...Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

3.10. All applications should therefore include an assessment of the risk of collateral intrusion and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed actions."

Unique Reference Number	

When completing this section, three points should be addressed:

Firstly, identify which third parties will be the subjects of collateral intrusion and what that intrusion will be i.e. what information will be captured about them?

Secondly, state why this is unavoidable. This could be because of the nature of the premises (e.g. a restaurant) or because of what the person is doing (e.g. visiting the subject/target premises). In some cases there will always be third parties around who will be captured on film or whose activities will be recorded/observed in some way.

Thirdly, set out what steps you have taken to minimise collateral intrusion, if this is possible. This may include:

- using a still camera rather than a video camera
- switching covert cameras on at specific times rather than leaving them to run all the time
- narrowing the field of vision or the place where the cameras are cited
- reducing the amount of surveillance done at busy times to capture fewer people e.g. when targeting shops or places of worship
- Pixelating the faces of people who are not targets if recordings are to be viewed by a wider audience e.g. a court

If you cannot minimise collateral intrusion you still need to show that you have considered it. In some situations all you may be able to state is that you cannot do anything to minimise collateral intrusion but you will not be making any decisions based upon the information gathered about third parties unless it shows them committing a criminal offence. Furthermore, you will ensure that officers who do the surveillance or view any recordings are mindful of who the real target of the surveillance is.

9. Explain <u>why</u> this directed surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means? [Code paragraph 3.4 to 3.7]

The Code of Practice contains detailed guidance on proportionality:

"3.4...This involves balancing the seriousness of the intrusion into the privacy of the target of the operation (or any other person who might be affected) against the need for the activity in investigative and operational terms."

" 3.5 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means."

Paragraph 3.6 requires you demonstrate that you have:

- balanced the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

Unique Reference Number	

- explained how and why the methods to be adopted will cause the least possible intrusion on the target and others;
- considered whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- evidenced, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

In order to comply with the above you need to address the following questions:

- Can you get information/evidence using less intrusive means/ overt methods?
- What other means have you tried to obtain the same information/evidence?
- What have you done to try and lessen the impact on the target? Factors to address include:
  - Amount of information to be gathered during surveillance
  - The method of surveillance e.g. using still cameras rather than video to capture less information or using one camera rather than two.
  - Impact of the surveillance on the subject
  - Timing of the surveillance

At the same time, the above must be balanced with the need for the activity in operational terms. To demonstrate this balance you should address:

- What you are seeking to achieve
- The seriousness and extent of the offence
- The impact of the offence on the victims (and others), the wider community and the public purse

For more guidance on proportionality see the examples on page 27 of the Code and also paragraph 106 of the OSC Document.

10. Confidential information. [Code paragraphs 4.1 to 4.31]
INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

This is defined in paragraph 4.1 of the Code as consisting of communications subject to legal privilege, communication between an MP and another person on constituency matters, confidential personal information and confidential journalistic material. So, for example, extra care should 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 matter should be reported to the OSC during the next inspection and the material should be made available to them if requested.

Local authorities are unlikely to come across this kind of information during routine surveillance operations. However you have to be alive to the possibility and include wording here to show you have thought about it. For example, where you will be following someone who may attend a church, mosque or hospital.

Note that in cases where you will be acquiring confidential information as part of a Directed Surveillance operation, the authorisation has to be granted by the Chief Executive or, in his or her absence, the acting Chief Executive.

Unique Reference Number	

11. Applicant's Details.			
Name (print)		Tel No:	
Grade/Rank		Date	
Signature			

12. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: *[Why is the surveillance necessary, Who is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

This section is for the Authorising Officer to complete. Authorising Officers should not normally be responsible for authorising operations in which they are directly involved. See paragraph 5.7 of the Code.

This section should not be pre completed by the Investigating Officer. Sufficient detail must be included here to demonstrate that the Authorising Officer has considered the application objectively. Reference can be made to the boxes completed by the Investigating Officer above but "cut and paste" should be avoided. The five "Ws" stated above must be addressed in detail. This is important so that the Investigating Officers are clear as to what they can and cannot do and the means they can adopt.

The Authorising Officer should also consider what is being authorised is not in conflict with previous or other current authorisations.

The Authorising Officer should not be afraid to reject the application if it lacks clarity or detail. Furthermore, the OSC Document recommends that if an application fails to include an element in the proposed activity which in the opinion of the Authorising Officer should have been included (for example, the return of something to the place from which it is to be taken for some specified activity), or which is subsequently requested orally by the Investigating Officer, it may be included in the authorisation; if so a note should be added explaining why. Conversely, if an Authorising Officer does not authorise all that was requested, a note should be added explaining why.

Unique Reference Number	

13. Explain <u>why</u> you believe the directed surveillance is necessary. [Code paragraph 3.3] Explain why you believe the directed surveillance to be proportionate to what is sought to be achieved by carrying it out. [Code paragraph 3.4 to 3.7]
The OSC Document (paragraph 105) states that the Authorising Officer should state why he/she believes that the Directed Surveillance is necessary and proportionate. A bare assertion is insufficient. You may refer to box 7 and 9 when completing this section. Set out what matters in the respective boxes you have given particular weight to when considering necessity and proportionality. You can also add any additional factors you have considered. To demonstrate that you have given the issues due thought, it is important not to "cut and paste" the Investigating Officer's wording or to just state "see box 7 and 9".

14. (Confidential Information Authorisation.) Supply detail demonstrating compliance with Code paragraphs 4.1 to 4.31				
Box 10 (above) explains Confidential Information. This box should only to be completed if you are likely to obtain Confidential Information through Directed Surveillance. If in doubt speak to the RIPA Co ordinator.				
Date of first review				
Programme for subsequent reviews of this authorisation: [Code paragraph 3.23]. Only complete this box if review dates after first review are known. If not or inappropriate to set additional review dates then leave blank.				
Reviews should be done as frequently as is considered necessary and practicable. The Code draws particular attention to the need to review authorisations frequently where the surveillance involves a high level of intrusion into private life or significant collateral intrusion, or where confidential information is likely to be obtained. During a review, consideration will have to be given to whether the surveillance is still necessary and proportionate. A standard form is available to record the review.				
Name (Print)		**Grade / Rank**	State the position of the Authorising Officer e.g. Director of Environmental Services	
Signature		**Date and time**		
According to the Code of Practice (paragraph 5.7), Authorising Officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons. Where an Authorising Officer authorises such an investigation or operation the Central Record should highlight this and the attention of the OSC should be drawn to it during the next inspection.				

Unique Reference Number	

Expiry date and time [e.g.: authorisation granted on 1 April 2005 - expires on 30 June 2005, 23.59]	All authorisations automatically last for three months. You cannot authorise for shorter periods. Even in the case of time limited surveillance operations you must cancel the authorisation as soon as the surveillance has been completed.

15. Urgent Authorisation [Code paragraphs 5.9]: Authorising officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given.

Paragraph 5.6 of the Code of Practice states:

"A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation 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 the urgency is of the authorising officer's own making."

In urgent cases this section still has to be completed as soon as reasonably practicable. It will be rare for a local authority to be able to claim that an authorisation was so urgent that it had to be obtained verbally. This is especially after 1st November 2012, when the requirement to seek a Magistrate's approval comes into force.

16. If you are only entitled to act in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully qualified authorising officer

This section is only to be completed where an urgent verbal authorisation was given by an Authorising Officer only entitled to act in urgent cases. This will usually not be appropriate for local authorities (see above).

Name (Print)		**Grade/ Rank**	
Signature		**Date and Time**	
Urgent authorisation Expiry date:		**Expiry time:**	
Remember the 72 hour rule for urgent authorities - check Code of Practice.	e.g. authorisation granted at 5pm on June 1st expires 4.59pm on 4th June		

WHAT NEXT?

The Directed Surveillance cannot be undertaken until a Magistrate has approved the authorisation. See part 5 of this document for the procedure for seeking such approval.

Once the authorisation has been approved a copy of this form (together with the Magistrates's Order) must be sent to the SRO or his/her designated representative so that he/she can update the Central Record.

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000
Review of a Directed Surveillance authorisation

Sample Form with Notes to Assist Completion

Regular reviews of all Directed Surveillance authorisations should be undertaken to assess whether they should continue or whether the criteria, upon which the original decision to grant an authorisation was based, have changed sufficiently to require the authorisation to be revoked. Before completing this form please read the Code of Practice (paragraph 3.22 - 3.26). Unlike authorisations and renewals of Directed Surveillance, a review does not have to be approved by a Magistrate.

Reviews should be done as frequently as is considered necessary and practicable. The Code draws particular attention to the need to review authorisations frequently where the surveillance involves a high level of intrusion into private life or involves significant collateral intrusion, or where confidential information is likely to be obtained.

The actual review is the responsibility of the original Authorising Officer and should, as a matter of good practice, be conducted by them or, failing that, by an officer who would be entitled to grant a new authorisation in the same terms. Support staff and Investigating Officers can though do the necessary research, prepare the review process and complete this form up to box 8.

Code of Practice/Code: This is the RIPA Covert Surveillance Code of Practice.

Unique Reference Number (URN): This is a reference unique to each individual form but which also allows the form to be matched with other forms in the same investigation or which are issued by the same department. Some organisations devise a URN which comprises of the year, department initials, applicant initials and investigation number. In some cases the investigating department allocates the URN whilst in others this is done by the RIPA Co ordinator. There are no hard and fast rules.

Public Authority *(including address)*			
Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Operation Name		**Operation Number*** *Filing Ref	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
		Review Number	

The above is self-explanatory. An additional requirement is an Operation Number. This is normally used for specific to police procedures. Local authorities may decide to just use the Unique Reference Number.

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000
Renewal of a Directed Surveillance Authorisation

Sample Form with Notes to Assist Completion

(Please attach a copy of the original authorisation.)

This form is to be completed by an officer of the local authority when the original authorisation period has expired but Directed Surveillance is still required. An application for renewal should not be made until shortly before the original authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. However the renewal has to be approved by a Magistrate in the same way the original authorisation was. If this is done, the authorisation will last for a further period of three months.

Code of Practice/Code: This is the revised RIPA Covert Surveillance Code of Practice.

Unique Reference Number (URN): This is a reference unique to each individual form but which also allows the form to be matched with other forms in the same investigation or which are issued by the same department. Some organisations devise a URN which comprises of the year, department initials, applicant initials and investigation number. In some cases the investigating department allocates the URN whilst in others this is done by the RIPA Co ordinator. There are no hard and fast rules.

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Renewal Number	This should be a sequential number reflecting the number of times this particular Directed Surveillance authorisation has been renewed.		

Unique Reference Number	

Details of renewal:

1. Renewal numbers and dates of any previous renewals.

Renewal Number	Date

2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.

Has anything changed in the way the surveillance is going to be carried out e.g. different premises targeted, different times when it will be done or equipment used etc.?

Has more information come to light reflecting greater need for surveillance e.g. seriousness of the offence, new victims, new witnesses etc.?

3. Detail the reasons why it is necessary to continue with the directed surveillance.

Set out how far you have achieved the desired objective. What more information is required?

Are you still investigating a criminal offence which meets the criteria set out in the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 i.e. a crime punishable with maximum term of at least 6 months imprisonment, or one which involves the sale of tobacco and alcohol to underage children?

You may refer to box 7 of the original authorisation application form and state what has or has not changed. See also the notes for that box for more guidance on necessity.

4. Detail why the directed surveillance is still proportionate to what it seeks to achieve.

You may refer to box 9 of the original authorisation application form and state what has or has not changed. See also the notes for that box for more guidance on proportionality.

State any further considerations which show that Directed Surveillance is still proportionate. In the light of the surveillance done so far, will you do things differently to ensure proportionality. e.g. reduce the times of surveillance or use different equipment?

5. Indicate the content and value to the investigation or operation of the information so far obtained by the directed surveillance.

This box requires you to review the information you have obtained so far by doing Directed Surveillance. It may be useful to refer to any review forms completed in relation to this surveillance.

Unique Reference Number	

6. Give details of the results of the regular reviews of the investigation or operation.			
This box requires you to look back at the review forms completed during the duration of the original authorisation that you are seeking to renew. You may wish to attach copies of the review forms or quote their unique reference numbers.			
7. Applicant's Details			
Name (Print)		**Tel No**	
Grade/Rank		**Date**	
Signature			

8. Authorising Officer's Comments. This box must be completed.			
The Authorising Officer should set out here why he/she believes that the original authorisation should be renewed taking care to explain the necessity (box 3) and proportionality (box 4) considerations. Reference can be made to the original authorisation application form for assistance, as many of the original considerations may still be relevant.			
9. Authorising Officer's Statement.			
I, [insert name], hereby authorise the renewal of the directed surveillance operation as detailed above. The renewal of this authorisation will last for 3 months unless renewed in writing. This authorisation will be reviewed frequently to assess the need for the authorisation to continue.			
Name (Print)		**Grade / Rank**	
Signature		**Date**	
Renewal From: **Time:**		**Date:**	
Date of first review.			
Date of subsequent reviews of this authorisation.			

Do not forget to set review dates. Reviews should be done as frequently as is considered necessary and practicable. The Code draws particular attention to the need to review authorisations frequently where the surveillance involves a high level of intrusion into private life or significant collateral intrusion, or where confidential information is likely to be obtained. During a review, consideration will have to be given to whether the surveillance is still necessary and proportionate. A standard form is available to record the review.

WHAT NEXT?

This renewal will not take effect until a Magistrate has approved it. See part 5 of this document for procedure for seeking such approval.

Once the renewal has been approved a copy of this form (together with the Magistrates's Order) must be sent to the SRO or his/her designated representative so that he/she can update the Central Record.

Unique Reference Number	

Part II of the Regulation of Investigatory Powers Act 2000

Cancellation of a Directed Surveillance authorisation

Sample Form with Notes to Assist Completion

This form is to be completed when cancelling an authorisation for Directed Surveillance. It is a statutory requirement that an authorisation is cancelled as soon as it is no longer required or no longer meets the criteria upon which it was authorised. Even where surveillance was conducted for a short time, the authorisation must be cancelled at the end of the operation. Authorisations cannot be left to just lapse. The Authorising Officer who granted or last renewed the authorisation must cancel it. Where that officer is no longer available, this duty will fall on the person who has taken over that role or the person who is acting as such. Unlike authorisations and renewals of Directed Surveillance, a cancellation does not have to be approved by a Magistrate.

Code of Practice/Code: This is the revised RIPA Covert Surveillance Code of Practice.

Unique Reference Number (URN): This is a reference unique to each individual form but which also allows the form to be matched with other forms in the same investigation or which are issued by the same department. Some organisations devise a URN which comprises of the year, department initials, applicant initials and investigation number. In some cases the investigating department allocates the URN whilst in others this is done by the RIPA Co ordinator. There are no hard and fast rules.

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch /Division**	
Full Address			
Contact Details			
Investigation /Operation Name (if applicable)			

Unique Reference Number	

Details of cancellation:			
1. Explain the reason(s) for the cancellation of the authorisation:			
This section is self explanatory. Reasons could include: "It is no longer necessary; we have obtained all the information we need." "It is no longer proportionate; the intrusion into the suspect's private life cannot be justified." "We do not have the resources to continue." "This was a short time limited operation." "The three month time limit has expired and we have decided to use other investigation methods."			
2. **Explain the value of surveillance in the operation:**			
State what actual surveillance was carried out under the authorisation. Explain what was achieved through the surveillance including information acquired as well as any surveillance product e.g. photographs, recordings etc. How is the surveillance product being stored, destroyed or otherwise handled? (see paragraphs 9.3 to 9.5 of the Code) How does the information/surveillance product assist with your investigation/prosecution? You may wish to look back at the original authorisation application form for this surveillance, in particular box 2 and box 5.			
3. **Authorising officer's statement.**			
I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above. Also include here directions to the Investigating Officers for the management and storage of the product of the surveillance e.g. photographs and other evidence. See paragraph 9.3 to 9.5 of the Code.			
Name (Print)		**Grade**	
Signature		**Date**	
4. **Time and Date of when the authorising officer instructed the surveillance to cease.**			
Date:		**Time:**	
It is important to formally instruct Investigating Officers to immediately cease any surveillance which is still ongoing and record that fact here and in the Central Record.			
5. Authorisation cancelled	**Date:**		**Time:**

Note: Once an authorisation has been cancelled, a copy of this form must be sent to the RIPA Co-coordinator so that she/he can update the Central Record.

APPENDIX 2
Forms for CHIS *(with notes to assist completion)*

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000
Application for authorisation of the conduct or use of a Covert Human Intelligence Source (CHIS)

Sample Form with Notes to Assist Completion

This form is to be completed by an officer of the local authority seeking authorisation for the deployment of a CHIS. Before completing it please read chapter 2 of the CHIS Code of Practice and chapter 6 (to understand the procedures that need to be in place to manage the CHIS). Once completed, this form should be forwarded to the Authorising Officer for approval and to complete box 13 onwards. The next step is to seek the approval of a Magistrate. If this is granted, the authorisation will last for twelve months.

Code of Practice/Code: The Covert Human Intelligence Sources Code of Practice.

Unique Reference Number (URN): This is a reference unique to each individual form but which also allows the form to be matched with other forms in the same investigation or which does the same department issue. Some organisations devise a URN which comprises of the year, department initials, applicant initials and investigation number. In some organisations the RIPA Co ordinator allocates the URN.

Public Authority *(including full address)*			
Name of Applicant		**Service/Department/ Branch**	
How will the source be referred to? i.e. what will be his/her pseudonym or reference number		You need to consider whether it is appropriate to use a pseudonym for the CHIS where the operation involves the CHIS being placed in a dangerous situation e.g. a CHIS who is part of a gang engaging in anti social behaviour on a housing estate. In other cases the use of the real name or reference number will suffice.	
The name, rank or position of the person within the relevant investigating authority who will have day to day responsibility for dealing with the source, including the source's security and welfare. (Often referred to as the Handler)		This is a requirement of the Act (S.29(5)(a) and the Code (paragraph 6.7). The Handler will usually be someone below the rank or position of the Authorising Officer. His/her job will include giving tasks to the CHIS e.g. to make a series of test purchases from a shop etc.	
The name, rank or position of another person within the relevant investigating authority who will have general oversight of the use made of the source. (Often referred to as the Controller)		This is the person referred to in Act (section 29(5)(b)) who will be responsible for the management and supervision of the Handler and the general oversight of the use made of the CHIS.	
Who will be responsible for retaining (in secure, strictly controlled conditions, with need-to-know access) the source's true identity, a record of the use made of the source and the particulars required under RIP (Source Records) Regulations 2000 (SI 2000/2725)?		This is the person in your organisation who maintains the Source Records in accordance with the Code (chapter 7) and the stated Regulations.	
Investigation/Operation			
Name (if applicable)			

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

DETAILS OF APPLICATION

1. Give rank or position of authorising officer in accordance with the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010; No.521 [1] *Where appropriate throughout amend references to the Order relevant to your authority.*

Insert the name and position of the Authorising Officer. This is the person who will decide whether or not the deployment of a CHIS should be authorised and will countersign this form. He/she must hold a rank in accordance with the above Order (i.e. Director, Head of Service, Service Manager or equivalent). Each department, which makes regular use of a CHIS, will have officers appointed as such. Care should be taken to avoid more junior officers signing authorisations. If in doubt consult the RIPA Co ordinator.

Please note where the CHIS operation involves the acquisition of confidential information (see box 11) or where the CHIS is a vulnerable individual (as defined in paragraph 4.22 of the Code) or a juvenile source (as defined in paragraph 4.23 of the Code) then this authorisation can only be granted by the Chief Executive or, in his/her absence, the acting Chief Executive.

2. Describe the purpose of the specific operation or investigation.

Explain the crime or disorder, which is being investigated. For example;

- "To investigate acts of vandalism and antisocial behaviour on X Housing Estate"
- "To investigate and gather evidence of the supply of meat unfit for human consumption [brief details]"
- "To investigate the operation of an illegal fly tipping business [brief details]"
- "To investigate the sale of dangerous goods to children in X Market"

If possible, include the relevant legislation that may be used to prosecute offenders and/or which gives you the power/duty to investigate the crime or disorder.

3. Describe in detail <u>the purpose</u> for which the source will be tasked or used.

What are you hoping to achieve by deploying the CHIS? For example:

- "To ascertain the extent of the suspect's alleged trade in clocked cars and who his suppliers are"
- "To collect evidence of drug dealing and noise nuisance on X Housing Estate"

Some background information about the investigation may be included to give the Authorising Officer an understanding of the context of the CHIS operation.

4. Describe in detail the proposed covert conduct of the source or <u>how</u> the source is to be used.

[1] For local authorities: The formal position of the authorising officer should be given. For example, Head of Trading Standards.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

Your statement here needs to include what activities the CHIS will be tasked with to fulfil the purpose set out in box 3. Points to address here include:

- What the CHIS will do e.g. "to pretend to be a new tenant on X Housing Estate with a view to obtaining information about drug dealing from local residents by forming relationships with them."
- Where are they going to do it?
- How long will the task last?
- When are they going to do it?
- Which premises are to be used and/or targeted?
- What type of equipment is going to be used e.g. hidden camera or microphone on the CHIS?

Note that if the Authorising Officer approves the deployment of the CHIS then the authorisation will only cover you to deploy the CHIS as stated here (subject to any amendments made by the Authorising Officer in box 13). Consequently you can rely on section 27 ("the RIPA Shield/Defence") only in so far as the CHIS was undertaking the activities set out in this section. Therefore it pays to be detailed in this section.

If you are using more than one CHIS in an operation, state the URN of that other authorisation here.

5. Identify on which grounds the conduct or the use of the source is necessary under Section 29(3) of RIPA. *Delete those that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on. (e.g. SI 2010 No.521)*

- ~~In the interests of national security;~~
- For the purpose of preventing or detecting crime or of preventing disorder;
- ~~In the interests of the economic well-being of the United Kingdom;~~
- ~~In the interests of public safety;~~
- ~~for the purpose of protecting public health;~~
- ~~for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department.~~

Local authorities can only authorise the use or conduct of a CHIS for the purpose of preventing or detecting crime or of preventing disorder. Therefore all other grounds should be deleted. If you believe that the deployment of the CHIS does not come under this heading then stop and seek advice from your legal department and/or the RIPA Co ordinator.

6. Explain why this conduct or use of the source is necessary on the grounds you have identified [Code paragraph 3.2]

The Authorising Officer must be satisfied that there is a necessity to use a CHIS in the proposed operation. You should explain here:

- What crime or disorder you are investigating.
- How the use of the CHIS lead to prevention or detection of that crime or prevention of that disorder
- Any other evidence you have to link the target with the offender/offence which requires corroboration through use of the CHIS

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

7. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 3.8 to 3.11.] Describe precautions you will take to minimise collateral intrusion and how any will be managed.

When deploying a CHIS you may be invading the privacy of those who are not your target e.g. customers at a shop, friends or relatives of the target. RIPA requires you to think about their rights and what you can do to minimise the impact of your surveillance on them.

The Code of Practice states:

"3.9 ...Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this collateral intrusion is considered proportionate to the aims of the intended intrusion. Any collateral intrusion should be kept to the minimum necessary to achieve the objective of the operation.
3.10. All applications should therefore include an assessment of the risk of any collateral intrusion and details of any measures taken to limit this, to enable the authorising officer fully to consider the proportionality of the proposed use or conduct of a CHIS."

People who may be the subject of collateral intrusion include:

- customers or workers at business premises
- visitors to a property
- friends or relatives of the suspect or person with whom the CHIS has formed a relationship

Firstly, identify whose privacy may be invaded by the deployment of the CHIS.

Secondly, state why it is unavoidable. This could be because of the nature of the premises (e.g. restaurant) or because of what the person is doing (e.g. visiting the target); there will always be third parties present who will not know that the CHIS is there for a covert purpose or that their activities are being recorded/observed in some way.

Thirdly, set out what steps (if any) you have taken to minimise collateral intrusion and how this will be managed. This may include:

- If the CHIS is to visit public premises (e.g. a restaurant or a retail outlet) he/she will only do so at less busy times to ensure fewer customers' privacy is invaded
- If the CHIS will be using a hidden microphone he/she will only switch it on when the target is present

If you cannot minimise collateral intrusion you still need to show you have considered it. You may wish to add that you cannot do anything to minimise it but you will not be making any decisions based on the information gathered about third parties unless it shows them committing a criminal offence. You must also remind your officers of the purpose and target of the surveillance and the need to keep information about third parties confidential.

8. Are there any particular sensitivities in the local community where the source is to be used? Are similar activities being undertaken by other public authorities that could impact on the deployment of the source? (see Code 3.17 and 3.18)

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

This section is probably more relevant to the police, given the extent of their use of CHIS and the wide ranging nature of investigations in which they are involved. The Code of Practice states:

"...3.17. Any person granting or applying for an authorisation will also need to be aware of any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS.

3.18. It is therefore recommended that where an authorising officer from a public authority considers that conflicts might arise they should, where possible, consult a senior officer within the police force area in which the CHIS is deployed. All public authorities, where possible, should consider consulting with other relevant public authorities to gauge community impact."

Are there any sensitivities of the local community that you need to record e.g. using a CHIS who may attend a place of worship? Are you aware of any similar investigations by the police or other local authorities which could have an impact here? Often you will only know this if the police or other local authorities inform you.

9. Provide an assessment of the risk to the source in carrying out the proposed conduct. (see Code 6.14. to 6.16)

You could be putting the CHIS in danger because of the task that you give him/her e.g. tasking a drug user to obtain information about drug dealers. Paragraph 6.14 of the Code of Practice states:

"Any public authority deploying a CHIS should take into account the safety and welfare of that CHIS when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a CHIS, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS, after the cancellation of the authorisation, should also be considered at the outset. Also, consideration should be given to the management of any requirement to disclose information tending to reveal the existence or identity of a CHIS to, or in, Court."

State here what health and safety risks are involved in deploying the CHIS and how you have addressed them e.g. personal security, panic alarm, use of fake identities, presence of other officers in the vicinity etc. Where you are deploying more than one CHIS in an operation you can still use one authorisation form but a separate risk assessment must be carried out in relation to each individual CHIS.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

10. Explain <u>why</u> this conduct or use of the source is proportionate to what it seeks to achieve. How intrusive might it be on the subject(s) of surveillance or on others? How is this intrusion outweighed by the need for a source in operational terms, and could the evidence be obtained by any other means? [Code paragraph 3.3 to 3.5]

This requires you to justify the need for using the CHIS and balance that with the impact on the privacy of the subject and others. The Ministry of Justice Guide on Human Rights states:

"When taking decisions that may affect any of the qualified rights, a public authority must interfere with the right as little as possible only going as far as is necessary to achieve the desired aim."

The Code of Practice explains proportionality as follows:

"3.3...This involves balancing the seriousness of the intrusion into the private or family life of the target of the operation (or any other person who might be affected) against the need for the activity in investigative and operational terms."

" 3.4 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the use or conduct of a CHIS proportionate. Similarly, an offence may be so minor that any deployment of a CHIS would be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means."

Paragraph 3.5 of the Code of Practice requires you to demonstrate that you have:

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

To demonstrate proportionality, the following issues must be addressed here:

- Can you get information using less intrusive means/ overt methods?
- What other means have you tried?
- What have you done to try and lessen the impact on the target? Factors to set out:
  - Amount of information to be gathered
  - Impact on the target
  - Timing of the surveillance

At the same time, the above must be balanced with the need for the deployment of the CHIS in operational terms. To demonstrate this balance you should set out:

- What you are seeking to achieve?
- Seriousness of the offence/disorder
- Impact of the offence/disorder on the victims
- Impact of the offence/disorder on others including the wider community and on the public purse

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

11. Confidential information. [Code paragraphs 4.1 to 4.21] Indicate the likelihood of acquiring any confidential information.

This is defined in paragraph 4.1 of the Code as consisting of communications subject to legal privilege, communication between an MP and another person on constituency matters, confidential personal information and confidential journalistic material. So, for example, extra care should 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 matter should be reported to the OSC during the next inspection and the material should be made available to them if requested.

Local authorities are unlikely to come across this kind of information during routine CHIS operations. However you have to be alive to the possibility and include adequate wording here to show you have thought about it. For example, where your CHIS may attend a church, mosque or doctor's surgery.

Note that in cases where you will be acquiring confidential information as part of a CHIS operation, the authorisation has to be granted by the Chief Executive or, in his/her absence, the acting Chief Executive.

References for any other linked authorisations:

12. Applicant's Details.

Name (print)		**Grade/Rank/Position**	
Signature		**Tel No**	
Date			

13. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW – in this and the following box]. The authorisation should identify the pseudonym or reference number of the source, not the true identity.

This section is for the Authorising Officer to complete. Please note that where the CHIS operation involves the acquisition of confidential information (see box 11 above) or where the CHIS is a vulnerable individual (as defined in paragraph 4.22 of the Code) or a juvenile source (as defined in paragraph 4.23 of the Code) then this authorisation can only be granted by the Chief Executive or in his/her absence the acting Chief Executive.

This section should not be pre completed by the Investigating Officer. Sufficient detail must be included here to demonstrate that the Authorising Officer has considered the application thoroughly. Reference can be made to box 3 and 4 above but "cut and paste" should be avoided.

The five "Ws" stated above must be addressed in detail. This is important so that the Investigating Officers and the CHIS are clear as to what they can and cannot do and the means they can adopt.

You, as the Authorising Officer, should not be afraid to reject the application if it lacks clarity or detail.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

14. Explain <u>why</u> you believe the conduct or use of the source is necessary. [Code paragraph 3.2] Explain <u>why</u> you believe the conduct or use of the source to be proportionate to what is sought to be achieved by their engagement. [Code paragraph 3.3 to 3.5]

You may refer to box 6 to 10 when completing this section. You can also add any additional factors you have considered. However, to demonstrate that you have given the issues due thought, it is important not to cut and paste that wording or to just state "see boxes 6 to 10".

The CHIS Handler is responsible for bringing to the attention of the CHIS Controller any concerns about the personal circumstances of the CHIS, insofar as they might affect:

- the validity of the risk assessment;
- the conduct of the CHIS;
- the safety and welfare of the CHIS.

Where appropriate, concerns about such matters must be considered by the Authorising Officer, and a decision taken on whether or not to allow the authorisation to continue.

15. (Confidential Information Authorisation.) Supply details demonstrating compliance with Code paragraphs 4.1 to 4.21

This box should only to be completed if you are likely to obtain Confidential Information (see box 11) through use of the CHIS. Note that in such cases the authorisation has to be granted by the Chief Executive or, in his/her absence, the Acting Chief Executive.

16. Date of first review	

17. Programme for subsequent reviews of this authorisation: [Code paragraphs 5.15 and 5.16]. Only complete this box if review dates after first review is known. If not, or inappropriate to set additional review dates, and then leave blank.

Regular reviews are stressed by the Code of Practice. Where a CHIS operation is going to last more than one month, the OSC has suggested that there should be a review once a month. Shorter or time limited operations may not require a review.

During a review, consideration will have to be given to whether the use of the CHIS is still necessary and proportionate. A standard form is available to record the review.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

18. Authorising Officer's Details			
Name (Print)		Grade/Rank/Position	
Signature		Time and date granted*	
		Time and date authorisation ends	Please note that all CHIS authorisations automatically last for twelve months. You cannot authorise for shorter periods. In the case of time limited CHIS operations you must cancel the authorisation as soon as the operation has been completed.

Authorising Officers should, where possible, be independent of the investigation. The Code states (paragraph 5.8), they should not normally be responsible for authorising their own activities e.g. those in which they themselves are to act as the CHIS or as the handler of the CHIS. However it is recognised that it is not always possible, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons. Where an Authorising Officer authorises his own activity, the Central Record should highlight this and the OSC should be about it during the next inspection.

* ***Remember, an authorisation must be granted for a 12 month period, i.e. 1700 hrs 4th June 2006 to 2359 hrs 3 June 2007***

19. Urgent Authorisation [Code paragraphs 5.13 to 5.14]: Authorising Officer: explain why you considered the case so urgent that an oral instead of a written authorisation was given
The Code of Practice states: "5.5 The authorising officer must give authorisations in writing, except that in urgent cases, they may be given orally. In such cases, a statement that the authorising officer has expressly authorised the action should be recorded in writing by the applicant (or the person with whom the authorising officer spoke) as a priority... 5.7 A case is not normally to be regarded as urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the operation or 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 the urgency is of the authorising officer's own making." In urgent cases this section still has to be completed as soon as reasonably practicable. It will be rare for a local authority to be able to claim that an authorisation was so urgent that it had to be obtained verbally. This is especially after 1st November 2012, when the requirement to seek a Magistrate's approval comes into force.

CHIS Unique Reference Number (URN) (to be supplied by the central monitoring officer).	

20. If you are entitled to act only in urgent cases: explain why it was not reasonably practicable for the application to be considered by a fully designated Authorising Officer
This section is only to be completed where an urgent verbal authorisation was given by an Authorising Officer only entitled to act in urgent cases. This will not be appropriate for local authorities (see above).

21. Authorising Officer of urgent authorisation				
Name (Print)		**Grade/Rank/Position**		
Signature		**Date and Time**		
Urgent authorisation expiry date:		**Expiry time:**		

Remember the 72 hour rule for urgent authorisations – check Code of Practice [Code Paragraph 4.18].
e.g. authorisation granted at 1700 on 1st June 2006 expires 1659 on 4th June 2006

WHAT NEXT?

The CHIS cannot be deployed until a Magistrate has approved the authorisation. See part 5 of this document for the procedure for seeking such approval.

Once the authorisation has been approved a copy of this form (together with the Magistrates's Order) must be sent to the SRO or his/her designated representative so that he/she can update the Central Record.

CHIS Unique Reference Number (URN)	

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000
Review of a Covert Human Intelligence Source (CHIS) authorisation

Sample Form with Notes to Assist Completion

Regular reviews of all CHIS authorisations should be undertaken to assess whether they should continue or whether the criteria upon which the original decision to grant an authorisation was based have changed sufficiently to require the authorisation to be revoked. Before completing this form please read the Code of Practice (paragraphs 3.12 - 3.16 and 5.15 - 5.16).

Reviews should be done as frequently as is considered necessary and practicable. The Code draws particular attention to the need to review authorisations frequently where the CHIS operation involves a high level of intrusion into private life or significant collateral intrusion, or where confidential information is likely to be obtained.

The actual review is the responsibility of the original Authorising Officer and should, as a matter of good practice, be conducted by them or, failing that, by an officer who would be entitled to grant a new authorisation in the same terms. Support staff and Investigating Officers can though do the necessary research, prepare the review process and complete this form up to box 8. Please refer to the original CHIS authorisation application form for more guidance on the definitions and principles, which are exactly the same here. A review does not have to be approved by a Magistrate.

Code of Practice/Code: The Covert Human Intelligence Sources Code of Practice.

Unique Reference Number (URN): This is a reference unique to each individual form but which also allows the form to be matched with other forms in the same investigation or which does the same department issue. Some organisations devise a URN which comprises of the year, department initials, applicant initials and investigation number. In some cases the investigating department allocates the URN whilst in others this is done by the RIPA Co ordinator. There are no hard and fast rules.

Public Authority *(including full address)*			
Applicant		**Unit/Branch**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Operation Name		**Operation Number*** *Filing Ref	
Date of authorisation or last renewal		**Expiry date of authorisation or last renewal**	
		Review Number	

CHIS Unique Reference Number (URN)	

Details of review:	
1. Review number and dates of any previous reviews.	
Review Number	**Date**
	If this review is part of a series of reviews then the date and number(s) of the previous review(s) must be inserted.
2. Summary of the investigation/operation to date, including what information has been obtained and the value of the information so far obtained.	
Summarise what has been done so far. You may wish to attach extracts of the Source Records. Set out what information you have obtained so far by deploying the CHIS. You also need to bring to the attention of the Authorising Officer any proposed or unforeseen changes to the nature or extent of the CHIS operation that may result in the further or greater intrusion into the private life of any person. Any such changes must also be highlighted at the next renewal if the authorisation is to be renewed.	
3. Detail the reasons why it is necessary to continue with using a Covert Human Intelligence Source.	
What more information is required? You may refer to box 6 of the original authorisation application form (as well as the guidance notes relating to it) and state what has or has not changed.	
4. Explain how the proposed activity is still proportionate to what it seeks to achieve.	
You may refer to box 10 of the original authorisation application form (as well as the guidance notes) and state what has or has not changed. State any further considerations, which show that deployment of the CHIS is still proportionate. In the light of the use you have made of the CHIS thus far, will you do things differently to ensure proportionality e.g. reduce the times of surveillance or use different equipment?	
5. Detail any incidents of collateral intrusion and the likelihood of any further incidents of collateral intrusions occurring.	
For an explanation of collateral intrusion see the notes relating to box 7 of the original authorisation application form.	
6. Give details of any confidential information acquired or accessed and the likelihood of acquiring	

CHIS Unique Reference Number (URN)	

confidential information.

For an explanation of confidential information see the notes relating to box 11 of the original authorisation application form. Consider :

- Have you recorded information about third parties? If so what?
- Can you do things differently to avoid or further minimise the collateral intrusion?

7. Give details of the review of the risk assessment on the security and welfare of using the source.

See box 9 of the original authorisation application form. Do you need to take any additional measures to safeguard the security and welfare of the CHIS?

8. Applicant's Details

Name (Print)		**Tel No**	
Grade / Rank		**Date**	
Signature			

9. Review Officer's Comments, including whether or not the use or conduct of the source should continue?

As the reviewing officer, you should set out here why you believe that the original authorisation should continue taking care to explain the necessity and proportionality considerations. You may refer to the original authorisation application form for assistance, as many of the original considerations may still be relevant. You should also consider:

- whether any proposed changes to the CHIS operation are proportionate (bearing in mind any extra intended intrusion into privacy or collateral intrusion)
- whether you need to amend the original authorisation in the light of what you have read above e.g. reduce the timings of the surveillance or length of the operation etc.

You should make a recommendation to the Authorising Officer to cancel, continue with or amend the original authorisation.

10. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.

If you decide that the original authorisation should continue, explain your reasons here and, if need be, set a further review date (below) bearing in mind the length of the operation and its impact on the target.

Reference can be made to the original authorisation application form, for assistance, as many of the original considerations will be relevant. Any additional requirements in terms of deploying the CHIS (e.g. security and welfare measures) should also be stated here. If you decide the authorisation should be cancelled you should explain your reasons. The cancellation form must now be completed. You should also immediately issue instructions to Investigating Officers to stop any further use or conduct of the CHIS.

Name (Print)		**Grade / Rank**	

CHIS Unique Reference Number (URN)	

Signature		**Date**	
Date of next review:			

Regular reviews are stressed by the Code of Practice. Where a CHIS operation is going to last more than one month the OSC has suggested that there should be a review once a month. Shorter or time limited operations may not require a review.

NOTE: Once this form is completed, a copy should be sent to the person maintaining the Central Record so that it can be updated.

CHIS Unique Reference Number (URN)	

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Application for renewal of a Covert Human Intelligence Source (CHIS) Authorisation

Sample Form with Notes to Assist Completion

(Please attach the original authorisation.)

This form is to be completed by an officer of the local authority when the period of authorisation for a Covert Human Intelligence Source (CHIS) has expired but the deployment of the CHIS is still required. An application for renewal should not be made until shortly before the original authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Before completing this form please read the Code of Practice (paragraphs 3.12 - 3.16 and 5.17 - 5.22). The next step is to seek the approval of a Magistrate. If this is granted, the authorisation will be renewed for a further period of twelve months.

The actual renewal is the responsibility of the original Authorising Officer and should, as a matter of good practice, be conducted by them or, failing that, by an officer who would be entitled to grant a new authorisation in the same terms. Support staff and Investigating Officers can though do the necessary research, prepare the review process and complete this form up to box 9.

Once completed this form should be forwarded to the Authorising Officer for approval and to complete box 10 onwards. If granted, the authorisation will cover a further period of 12 months. Please refer to the CHIS authorisation application form for more guidance on the definitions and principles mentioned below.

Code of Practice/Code: The Covert Human Intelligence Sources Code of Practice.

Unique Reference Number (URN): This is a reference unique to each individual form but which also allows the form to be matched with other forms in the same investigation or which does the same department issue. Some organisations devise a URN, which comprises of the year, department initials, applicant initials and investigation number. In some cases the investigating department allocates the URN whilst in others this is done by the RIPA Co ordinator. There are no hard and fast rules.

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			
Renewal Number	This should be a sequential number reflecting the number of times this particular CHIS authorisation has been renewed.		

CHIS Unique Reference Number (URN)	

Details of renewal:	
1. Renewal numbers and dates of any previous renewals.	
Renewal Number	**Date**
2. Detail any significant changes to the information as listed in the original authorisation as it applies at the time of the renewal.	
Has anything changed in the way the CHIS is going to be used e.g. different premises targeted, different tasks to be given, different times or equipment used etc.? Has more information come to light reflecting greater need for the CHIS e.g. seriousness of the offence, new victims?	
3. Detail why it is necessary to continue with the authorisation, including details of any tasking given to the source.	
Is the investigation/operation continuing? What more information is required to be obtained by the CHIS? What have you achieved thus far? You may refer to box 6 of the original authorisation application form (as well as the guidance notes relating to it) and state what has or has not changed.	
4. Detail why the use or conduct of the source is still proportionate to what it seeks to achieve.	
You may refer to box 10 of the original authorisation application form (as well as the guidance notes which relate to it) and state what has or has not changed. State any further considerations, which show that deployment of the CHIS is still proportionate. In the light of the use you have made of the CHIS thus far, will you do things differently to ensure proportionality e.g. reduce the times of surveillance or use different equipment?	
5. Detail the use made of the source in the period since the grant of authorisation or, as the case may be, latest renewal of the authorisation.	
What use have you made of the CHIS so far? List dates, times and places and the nature of each use. You may attach extracts from the Source Records.	
6. List the tasks given to the source during that period and the information obtained from the conduct or use of the source.	
Similar to above - You may refer to the Source Records.	
7. Detail the results of regular reviews of the use of the source.	
This box requires you to look back at the review forms completed during the duration of the original authorisation that you are seeking to renew. You may wish to attach copies of those forms or include their unique reference numbers.	
8. Give details of the review of the risk assessment on the security and welfare of using the source.	
See box 9 of the original authorisation application form. Do you need to take any additional measures to safeguard the security and welfare of the CHIS?	

CHIS Unique Reference Number (URN)	

9. Applicant's Details			
Name (Print)		Tel No	
Grade/Rank		Date	
Signature			

10. Authorising Officer's Comments. This box must be completed.

The Authorising Officer should state here whether or not he/she is satisfied that the CHIS authorisation should be extended and the reasons for his/her decisions.

Any other special requirements for the deployment of the CHIS (e.g. security and welfare considerations) should also be stated here. In particular the Authorising Officer should consider necessity, proportionality, collateral intrusion and the risk assessment and state that he/she is satisfied with all the compliance measures in place. Reference can be made to box 3 and 4 as well as any other matters taken into account.

11. Authorising Officer's Statement. THE AUTHORISATION SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.

An example:

"I, [insert name], hereby authorise the renewal of the deployment of the CHIS [insert pseudonym or reference] as detailed above. The renewal of this authorisation will last for 12 months unless cancelled. This authorisation will be reviewed frequently to assess the need for it to continue."

Name (Print)		Grade / Rank	
Signature		Date	
Renewal From: Time:		Date: End date/time of the authorisation	

NB. Renewal takes effect at the time/date of the original authorisation would have ceased but for the renewal

Date of first review:	
Date of subsequent reviews of this authorisation:	

WHAT NEXT?

The renewal of the CHIS authorisation does not take effect until a Magistrate has approved the authorisation. See part 5 of this Policy and Procedural document for the procedure for seeking such approval.

Once the renewal has been approved a copy of this form (together with the Magistrates' Order) must be sent to the Senior Responsible Officer (SRO) or his/her designated representative so that he/she can update the Central Record.

CHIS Unique Reference Number (URN)	

Part II of the Regulation of Investigatory Powers Act (RIPA) 2000

Cancellation of an authorisation for the use or conduct of a Covert Human Intelligence Source

Sample Form with Notes to Assist Completion

This form is to be completed by an officer of the local authority when cancelling the authorisation of a Covert Human Intelligence Source (CHIS). It must be signed by the Authorising Officer.

It is a statutory requirement that an authorisation is cancelled as soon as it is no longer required or no longer meets the criteria upon which it was authorised. Even where a CHIS operation was conducted for a short time, the authorisation must be cancelled at the end of the operation. Authorisations cannot be left to just lapse. The Authorising Officer who granted or last renewed the authorisation must cancel it. Where that officer is no longer available, this duty will fall on the person who has taken over that role or the person who is acting as such. A cancellation does not have to be approved by a Magistrate.

Once completed this form should be forwarded to the Authorising Officer for approval and to complete box 3 onwards.

Code of Practice/Code: The Covert Human Intelligence Sources Code of Practice.

Unique Reference Number (URN): This is a reference unique to each individual form but which also allows the form to be matched with other forms in the same investigation or which does the same department issue. Some organisations devise a URN which comprises of the year, department initials, applicant initials and investigation number. In some cases the investigating department allocates the URN whilst in others this is done by the RIPA Co ordinator. There are no hard and fast rules.

Public Authority *(including full address)*			
Name of Applicant		**Unit/Branch**	
Full Address			
Contact Details			
Pseudonym or reference number of source			
Investigation/Operation Name (if applicable)			

CHIS Unique Reference Number (URN)	

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

This section is self explanatory. Reasons could include:

"It is no longer necessary; we have obtained all the information we need."
"It is no longer proportionate; the intrusion into the suspect's private life cannot be justified."
"We do not have the resources to continue."
"This was a short time limited operation."
"The twelve month time limit has expired and we have decided to adopt other means of investigation."

2. Explain the value of the source in the operation:

State what the CHIS was tasked to do under the authorisation. How does the information/surveillance product you have acquired though the deployment of the CHIS assist with your investigation/prosecution? You may wish to look at the original CHIS authorisation application form.

3. Authorising officer's statement. THIS SHOULD IDENTIFY THE PSEUDONYM OR REFERENCE NUMBER OF THE SOURCE NOT THE TRUE IDENTITY.

For example:
"I, [insert name], hereby cancel the authorisation of [insert pseudonym or reference number] as a CHIS for [name of authority] and require all officers to cease his/her deployment as such in any investigation/operation. "

Once cancelled you should also:

- formally instruct the investigating officers to immediately cease any use or conduct involving the CHIS
- issue any necessary instructions to ensure that the surveillance product (e.g. photographs, recordings etc.) are handled and stored properly (see paragraphs 8.1 to 8.3 of the Code)
- consider whether it is necessary to continue with the security and welfare arrangements for the CHIS

Name (Print)		**Grade**	
Signature		**Date**	

4. Time and Date of when the authorising officer instructed the use of the source to cease.

Date:		**Time:**	

NOTE: Once this form is completed, a copy should be sent to the person maintaining the Central Record so that it can be updated.

APPENDIX 3
Forms for Communication Data *()*

Form CD1

Chapter II of Part I of the Regulation of Investigatory Powers Act 2000 (RIPA)

Application for Communications Data

Form CD1

1) Applicant's Name		**4) Unique Reference Number**	
2) Office, Rank or Position		**5) Applicant's Telephone Number**	
3) Applicant's Email Address		**6) Applicant's Fax Number**	

7) Operation Name (if applicable)		**8) STATUTORY PURPOSE**
		S22 (2)(b) Prevention and Detection of Crime

9) COMMUNICATIONS DATA **Describe the communications data, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s)**

10) NECESSITY State the nature of the investigation or operation and how it relates to a purpose at question 8. *Give a short explanation of the crime (or other purpose), the suspect, victim or witness and the phone or communications address and how all these three link together*

11) PROPORTIONALITY **State why obtaining the communications data is proportionate to what you are seeking to achieve** *Outline what is expected to be achieved from obtaining the data and explain how the level of intrusion is justified when taking into consideration the benefit the data will give to the investigation. When considering the benefits to the investigation or operation can the level of intrusion be justified against the individual's right to privacy? Explain why you have requested the specific date/time periods i.e. how these are proportionate.*

12) COLLATERAL INTRUSION **Consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances** *If you have identified any meaningful degree of collateral intrusion, explain what it is.*

13) TIMESCALE **Identify and explain the timescale within which the data is required**	

14) APPLICANT **I undertake to inform the SPoC of any change in circumstances that no longer justifies the acquisition of the data**			
Applicant's Signature		**Date**	

15) ASSESSMENT BY ACCREDITED SPoC	
How much will the acquisition of the communications data cost	
Are there other factors the DP should be aware of? *For example the requirement:* • *Is NOT reasonably practicable for the CSP to do;* • *Will cause an adverse cost or resource implication to either your public authority or the CSP (for instance does the investigation or operation have the analytical capacity to undertake analysis of the communications data once acquired);* • *Will produce excess data to what is required.*	
Name of Accredited SPoC	

16) AUTHORISATION (Completed by Accredited SPoC when appropriate)	
Specify the reason why the collection of communications data by means of an authorisation is appropriate: ☐ There is an agreement in place between the public authority and the CSP relating to the appropriate mechanisms for the disclosure of the data; ☐ The designated person considers there is a requirement to identify to whom a service is provided (for example subscriber check) but a CSP has yet to be conclusively determined as the holder of the communications data; ☐ CSP is not capable of obtaining or disclosing the communication data	
Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought. **Describe the course of conduct required to obtain the data.**	☐ Service use data- acquisition by SPOC directly from CSP ☐ Subscriber information – acquisition by SPOC ☐ Other conduct - specify

The statutory purpose for which the conduct may be authorised is set out at section 8 of this form.

The office, rank or position of the designated person should be recorded within section 17 of this form, together with a record of the date & time the granting of an authorisation is made.

17) DESIGNATED PERSON			
The Designated Person considers the application and if approved records their considerations: • *Why do you* ***believe*** *acquiring the communications data is necessary for one of the purposes within section 22(2) of the Act;* • *Why do you* ***believe*** *the conduct involved in obtaining the data is proportionate to the objective(s)? In making that judgement you should take in consideration any additional information from the SPoC.* • *If the applicant has identified any meaningful degree of collateral intrusion, why you* ***believe*** *the request remains justified and proportionate to the objective(s)?*			
My considerations in approving/not approving this application are:			
☐ I authorise the conduct to be undertaken by the SPoC as set out in section 16 of this form ☐ I give Notice and require the SPoC to serve it on (**insert name of CSP)**. The Notice bears the unique reference number **(number)**			
Name		**Office, Rank or Position**	
Signature		**Time and Date**	

Form CD2

APPLICATION FOR COMMUNICATIONS DATA -
SPOC REJECTION FORM

SPOC Ref No.		**Application Ref No.**	

Applicant Name		**Rank / Grade**	
Department		*Other Ref (if relevant)*	

Your Application for communications data has been REJECTED FOR THE FOLLOWING REASONS:

Insufficient Information in relation to:

- ☐ **Nature of Enquiry / Investigation (Application Form Question 3)**
- ☐ **Source of Telephone Number / Other Data (Application Form Question 5)**
- ☐ **Necessity (Application Form Question 6)**
- ☐ **Proportionality (Application Form Question 7)**
- ☐ **Collateral Intrusion (Application Form Question 8)**

☐ **Subscriber / Account Details must be obtained before requesting Outgoing Call Data or Specialist Services**

☐ **The time / date period requested has not been adequately justified**

☐ **The request does not meet the criteria for this type of service. (Specify Reasons)**

☐ **The request has been refused by the Designated Person**

☐ **Other (Specify)**

The original copy of this application is held by the SPOC.

SPOC Name		*Date*	
Signature			

Form CD3

CANCELLATION OF NOTICE ISSUED UNDER SECTION 22 (4) (8) OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000

SPOC Ref No.		**Application Ref No.**		**URN of Notice**	

TO BE COMPLETED BY THE SPOC	
To CSP (full name & address)	
You are required to cancel the collection of communications data in respect of the above URN.	
Date/Time verbally advised to cease activity and by whom	
Telephone Number / or other Communications Data to which this cancellation relates:	
Details of Service / Data to be cancelled	

Designated Person Name and Rank/ Grade	
Date of requirement to cancel	

This cancellation may be verified by contacting the following:			
SPOC Name		**SPOC Telephone Number**	

NOTICE – Section 22(4) of the Regulation of Investigatory Powers Act 2000 (RIPA)

This form is sent to the CSP to request Communications Data- Form CD4

Where it appears to the designated person that a CSP is or may be in possession of, or be capable of obtaining, any communications data, the designated person may, by notice require the CSP –

(a) if the CSP is not already in possession of the data, to obtain the data; and
(b) in any case, to disclose all of the data in his possession or subsequently obtained by him.
S. 22(6) – It is the duty of the CSP to comply with any notice given to him under subsection (4).

Other SpoC Reference*		Unique Reference Number of Notice	
Details of the CSP	**Name of the CSP** **Address of CSP** **For attention of**		
Statutory Purpose	S22 (2)(b) Prevention and detection of crime		
Designated Person Giving Notice **This Notice is valid for one month when given by the Designated Person**	**Name of DP** **Office, rank or position** **Date Notice given** **and if appropriate the time**		
Describe the communications data to be acquired specifying, where relevant, any historic or future date and/or time periods sought.	**Data applied for** **Time period (if applicable)**		
DCG Grade 3 – SpoC may indicate any specific or critical time issues such as bail dates, court dates, persons in police custody, specific line of investigation in serious crime (S.81(2) RIPA) investigation and the acquisition of data will directly assist in the prevention or detection of the crime. URGENT (DCG Grade 1 or 2) may only be initiated by SpoC and may require liaison with CSP staff.	**DGC Grading Scheme: Grade 3/ Grade 3 Specific or Time Critical Issue** **Grade 3: If, and only if there is a specific or critical time issue state the 'target date' for the disclosure of the data** **Explain the reason for the setting of a target date** **Comment:** Ordinarily all Notices are Grade 3 and will be dealt with in date order when received by the CSP, DCG has requested the IOCCO Inspectors to make appropriate comment on the use of the grading scheme during their inspections of law enforcement agencies.		
Specify the manner in which the data should be disclosed	**By letter, e-mail or fax to:-**		
SpoC Office Contact Details and Address **If there is a specific or critical time issue indicated or the matter is DCG Grade 1 or 2 URGENT then the Accredited SpoC details MUST be completed**	**TEL** **FAX** **EMAIL** **POSTAL** **Name of Accredited SpoC** **Mob TEL** **Reminder: If you have requested a "24/7" response from the CSP make sure you supply sufficient contact details so that you and your SpoC colleagues can be easily contacted**		
Date Notice served **and if appropriate the time**			

[1] CSPs must ensure the data is returned to a verified SPOC e-mail or fax number. For information about how a CSP may verify the identity of a SPOC by the use of the SPOC PIN list, contact commsdata@homeoffice.gsi.gov.uk

For information about how a CSP may verify the identity of a SPOC by the use of the SPOC PIN list, contact commsdata@hoeoffice.gsi.gov.uk

Chapter II of Part I of the Regulation of Investigatory Powers Act 2002 (RIPA)

Reporting of an Error by Accredited SPOC - Form CD5

Name of Authority reporting this error: Cyngor Sir Ceredigion County Council

An error can only occur after a designated person:

- Has granted an authorisation and the acquisition of data ahs been initiated, or
- Has given notice and the notice has been served on a CSP in writing, electronically or orally.

1) Name of Accredited SPOC		**4) SPOC's Telephone Number**	
2) Office, Rank or Position of SpoC		**5) SPOC's Fax Number**	
3) SPOC's Email Address		**6) The error can be reported by email to**	**Ch2.inspectorate@homeoffice.gsi.gov.uk**

7) DETAILS OF THE ERROR
State whether Notice or Authorisation; Notice URN: - **Describe the communications data applied for as set out on the application;** **Describe the nature of the error;** **Date and time the error occurred; Date Time** **If the error was made by the CSP – Name of CSP; and state whether CSP has been informed.** **Yes:** **No: Include reason why CSP not informed:**
8) UNINTENDED COLLATERAL INTRUSION
If any has taken place, please describe what it was;
9) PREVENTION OF SIMILAR ERRORS REOCURRING
What steps have been, or will be, taken to ensure that a similar error does not reoccur
10) REPORTING OF THE ERROR TO THE COMMISSIONER AND NOTIFYING THE SENIOR RESPONSIBLE OFFICER AND THE DESIGNATED PERSON *Note; there is a requirement to report the error to your senior responsible officer (SRO) and then to the Commissioner*

Details of the SRO	**Name of the SRO** **Email address of SRO**	**Telephone No**
Details of the DP	**Name of the DP** **Email address of DP**	**Telephone No**
The date and time the report has been completed by SpoC	**Date**	**Time**

Form CD6

SPOC LOG SHEET – Form CD6

SPOC Reference Number		Unique Reference Number	

Telephone number/ e-mail or other address

1)	2)
3)	4)
5)	6)

Action	Summary of Enquiry (including time & date and CSP or other person to whom SPOC spoke or any other information which may be relevant to this case)	Name of SPOC
Date Application received by SPOC		
Date S22(4) notice(s) drafted and sent to DP for approval		
Date and URNs of notices served on CSP and how		
Details of any porting of number(s) by CSP		
Details of any contact by SPOC with applicant, CSP or DP (1)		
Details of any contact by SPOC with applicant, CSP or DP (2)		
Details of any contact by SPOC with applicant, CSP or DP (3)		
Details of any contact by SPOC with applicant, CSP or DP (4)		
Date results received from CSP		
Who was the result passed onto and in what format & at what time & date		

APPENDIX 4
Form for Applying for Judicial Approval *(with notes to assist completion)*

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.

Local authority:.....

Local authority department:.....

Offence under investigation[1]:.....

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 details[3]

.....

.....

.....

.....

.....

.....

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

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before
MAGISTRATE[4]:.....

Address of applicant department:.....

.....

Contact telephone number:.....

Contact email address (optional):.....

Local authority reference:.....

Number of pages:.....

Order 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.[5]

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.

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

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

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

Notes to Assist Completion

[1]Insert 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.

[2]You 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.

[3]This forms the basis of the application to the MAGISTRATE 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 no 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.

[5]The 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.

[6]If 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 your Legal Section and/or RIPA Co coordinator with regards to the next steps.

[7]If 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 your Legal Section and/or RIPA Co Coordinator with regards to the next steps.

CYNGOR SIR CEREDIGION COUNTY COUNCIL

NON – RIPA SURVEILLANCE

GUIDANCE FOR OFFICERS

April 2013

Cyngor Sir Ceredigion County Council

NON - RIPA SURVEILLANCE

Guidance for Officers draft 11.11.16

From time to time the Council may wish to undertake covert surveillance, which is not regulated by the Regulation of Investigatory Powers Act 2000 Part II (RIPA). This is fine, as RIPA is permissive legislation.

The 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.

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

Authorisation under RIPA affords a public authority a defence under Section 27 i.e. the activity is lawful for all purposes, provided an authorisation is in place, and the conduct of officers is in accordance with the legislation.

However, failure to obtain an authorisation does not make covert surveillance unlawful.

Section 80 contains a general saving for lawful conduct, and states:

"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."

Examples of Non-RIPA Surveillance
Below are examples of activity which does not meet the RIPA criteria/threshold

1) **Crimes Not Carrying Six Months Imprisonment**

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 (offences involving sale of tobacco and alcohol to underage children).

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."

2) Employee Surveillance

Most employee surveillance will not be authorisable under RIPA.

See 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.

Human Rights Compliance

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

Authorising Non-RIPA Surveillance
See Flowchart ***–Appendix A***

Authorising Officers include:

Deputy Chief Executive, Chief Finance officer/S151 Officer & Head of Lifestyle Services.

A URN should be sought from the Senior Responsible Officer prior to submission to Authorising Officers.

Copy forms should be sent to the SRO for entry in Central Register upon completion of authorisation process.

Data Protection Compliance

Section 1 of RIPA (unlawful interception) does not apply to Local authorities, except where the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000 (SI 2000/2699) applies.

The Telecommunications Regulations permits 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 Informations Security Policy.

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.

Data Protection Employment Practices Code of Practice

The Information Commissioner has published a **Data Protection Employment Practices Code of Practice (**available at www.ico.gov.uk) (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 which 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 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.
- 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.

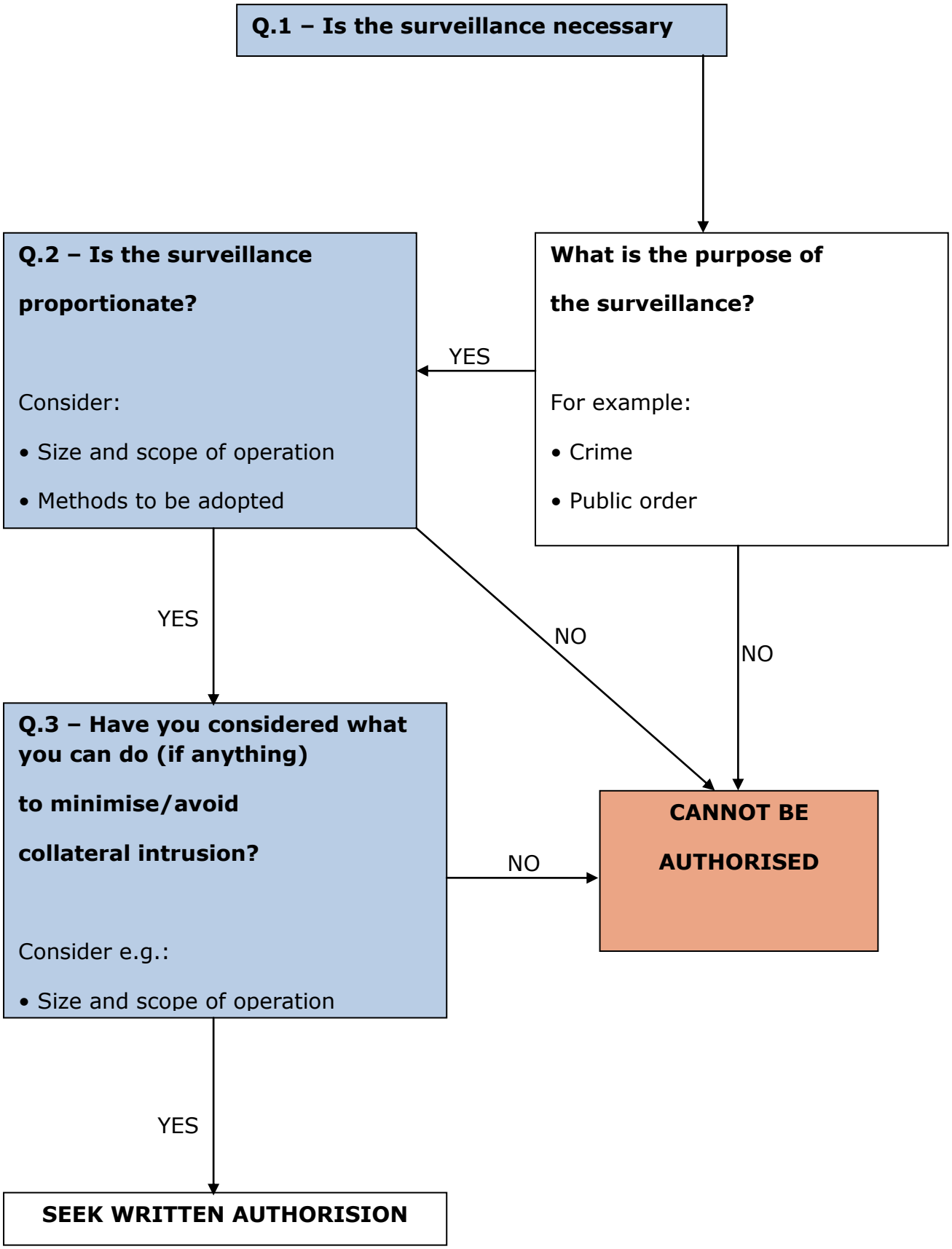
In both the above NON-RIPA cases it is important to have a proper audit trail through written records. In his annual report (2011/2012) the Chief Surveillance Commissioner (at paragraph 5.22) emphasised this:

"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."

Non-RIPA Authorisation Form
An example of a Non-RIPA authorisation form is shown at ***Appendix B***

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

Non-RIPA requests and authorisations will be the subject of 6-monthly reports by the Senior Responsible Officer (Monitoring Officer) to the Overview & Coordinating Scrutiny Committee


Q.1 – Is the surveillance necessary
What is the purpose of the surveillance?
For example:
• Crime
• Public order
YES
Q.2 – Is the surveillance proportionate?
Consider:
• Size and scope of operation
• Methods to be adopted
NO
YES
Q.3 – Have you considered what you can do (if anything) to minimise/avoid collateral intrusion?
Consider e.g.:
• Size and scope of operation
NO
CANNOT BE AUTHORISED
YES
SEEK WRITTEN AUTHORISION

Unique Reference Number	

Appendix B
Application for Authorisation to conduct Covert Surveillance not regulated by RIPA

Sample Form with Notes to Assist Completion

This form should be completed by an officer of the local authority seeking authorisation to carry out surveillance which **does not** fall within the definition of Directed Surveillance in section 28 of the Regulation of Investigatory Powers Act 2000 (RIPA).

This could include surveillance where the target is doing something which is not criminal offence ,or which does not carry a term of imprisonment of six months or more, misusing the work e mail/internet system or breaching a legal agreement (e.g. tenancy agreement).

Before completing this form please consult:

- The ICO Employment Practices Code: Part 3 (Staff Surveillance)

Once completed this form should be forwarded to your manager to complete box 11 onwards.

Organisation *(including full address)*			
Name of Applicant		**Department** **Section**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person other than the applicant)			

Unique Reference Number	

DETAILS OF APPLICATION

1. Give position of the authorising officer

This is the person who will decide whether or not the surveillance should be authorised and will countersign this form. It may be the Head of the Service carrying out the surveillance.

2. Describe the purpose of the specific operation or investigation.

Explain what is being investigated. For example:

- Minor offence
- Misuse of email/internet
- Inaccurate completion of timesheet
- Breach of a tenancy agreement

If possible, include the relevant legislation that which gives you the power/duty to investigate the matter and to take action.

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, and recorder) that may be used.

The key phrase is "in detail." Therefore a response which merely states **"**Video camera and recording equipment will be installed at a fixed point" will not be adequate.

Your statement here needs to include what is going to be done, who is going to do it, when they are going to do it, where they are going to do it and how they are going to do it. Other points to address here include:

- How long will the surveillance last?
- Specific details about dates and times i.e. is it 24/7, at specific times of the day or at random times?
- Which premises are to be used and/or targeted?
- Which vehicles are to be used? Are they public or private?
- What type of equipment is to be used? e.g. covert cameras, audio devices
- What is the capability of the equipment to be used? e.g. zoom lens, remote controlled etc.
- Who else will be involved in the operation and what will be their role? e.g. private detectives, police

It may be appropriate to attach plans/maps showing where and how the surveillance will be conducted and indicating where any surveillance equipment will be installed.

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

Include as much information as you have. If you do not know the identity of the target(s) then say so. You could include a general description of the target(s).

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

Your statement here should be more detailed than in Box 2. You should give details of the precise information sought by doing the surveillance. For example:

- "To ascertain what time the employee enters and leaves the office."
- "To capture images of the employee making unauthorised visits to service users."
- "To find out what websites the employee has been visiting and what images have been downloaded."

6. Has any warning/notice been served on the target? If not, explain why this surveillance needs to be covert

The warning could be general one (e.g. signs/policy) or it could be more specific (e.g. letter).

Explain any overt methods you have tried to obtain the evidence/information or why they are not appropriate.

Explain the consequences of the target finding out about this surveillance.

7. Explain <u>why</u> this surveillance is necessary

Include in this box details of:

- Why surveillance is needed to obtain the information/evidence that is sought
- Any other means you have tried (not involving surveillance) to obtain the same information/evidence
- Any other evidence/information you have to link the target with the offender which requires corroboration through surveillance

8. **Supply details of any potential collateral intrusion and why the intrusion is unavoidable.** Describe precautions you will take to minimise collateral intrusion

When doing surveillance you may be invading the privacy of those who are not your target. You are required to think about their rights and what you can do to minimise the impact on them of your surveillance. People who may be the subject of collateral intrusion include:

- fellow employees
- visitors to a property
- friends or relatives of the suspect

When completing this section, three matters should be addressed:

Firstly, identify which third parties will be the subject of collateral intrusion and what that intrusion will be i.e. what information will be captured about them?

Secondly, state why this is unavoidable. This could be because of the nature of the premises (e.g. a restaurant) or because of what the person is doing (e.g. visiting the subject/target premises). In some cases there will always be third parties around who will be captured on film or whose activities will be recorded/observed in some way.

Thirdly, set out what steps you have taken to minimise collateral intrusion, if this is possible.

If you cannot minimise collateral intrusion you still need to show you have considered it. In some situations all you may be able to state is that you cannot do anything to minimise collateral intrusion but you will not be making any decisions based upon the information gathered about third parties unless it shows them committing a criminal offence. Furthermore, you will ensure that officers who do the surveillance or view any recordings are mindful of who the real target of the surveillance is.

9. Explain <u>why</u> this surveillance is proportionate to what it seeks to achieve. How intrusive might it be on the subject of surveillance or on others? And why is this intrusion outweighed by the need for surveillance in operational terms or can the evidence be obtained by any other means?

The RIPA Covert Surveillance Code of Practice contains detailed guidance on proportionality:

"3.4…This involves balancing the seriousness of the intrusion into the privacy of the target of the operation (or any other person who might be affected) against the need for the activity in investigative and operational terms."

"3.5 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected minor offence may be serious will not alone render intrusive actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity should be considered proportionate if the information which is sought could

reasonably be obtained by other less intrusive means."

Here you demonstrate that you have:

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

In order to comply with the above you need to address the following questions:

- Can you get information using less intrusive means/overt methods?
- What other means have you tried to obtain the same information/evidence?
- What have you done to try and lessen the impact on the target? Factors to address include:

  - Amount of information to be gathered during surveillance
  - The way the surveillance is done e.g. using still cameras rather than video to capture less information or using one camera rather than two.
  - Impact of the surveillance on the subject
  - Timing of the surveillance

At the same time, the above must be balanced with the need for the activity in operational terms. To demonstrate this balance you should address:

- What you are seeking to achieve?
- Seriousness and extent of the offence
- Impact of the offence on the victims, others/wider community and on the public purse

For more guidance on proportionality see the examples on page 17 of the RIPA Covert Surveillance Code and also paragraph 103 of the OSC Procedures and Guidance Document.

10. Applicant's Details.			
Name (print)		**Tel No:**	
		Date	

Position			
Signature			

11. Authorising Officer's Statement. [Spell out the "5 Ws" – Who; What; Where; When; Why and HOW– in this and the following box.]

I hereby authorise directed surveillance defined as follows: *[Why is the surveillance necessary, Who is the surveillance directed against, Where and When will it take place, What surveillance activity/equipment is sanctioned, How is it to be achieved?]*

This section is for the Authorising Officer to complete. Ensure that you are satisfied that any covert monitoring is strictly targeted at obtaining evidence within a set timeframe and that it does not continue after the investigation is complete.

Sufficient detail must be included here to demonstrate that you, as the Authorising Officer, have considered the application objectively. Reference can be made to the boxes completed by the Investigating Officer above but "cut and paste" should be avoided. The five "Ws" stated above must be addressed in detail. This is important so that the Investigating Officers are clear as to what they can and cannot do and the means they can adopt.

You should not be afraid to reject the application if it lacks clarity or detail.

12. Explain <u>why</u> you believe the surveillance is necessary.
Explain <u>why</u> you believe the surveillance to be proportionate to what is sought to be achieved by carrying it out.

You should satisfy yourself that there are grounds for suspecting criminal activity or equivalent malpractice and that notifying individuals about the monitoring would prejudice its prevention or detection. Set out what matters in the respective boxes you have given particular weight to when considering necessity and proportionality. You can also add any additional factors you have considered.

Date of first review	If the surveillance operation is going to last more than a month then you should consider whether it should be reviewed after a period of time. During a review, consideration will have to be given to whether the surveillance is still necessary and proportionate.

Programme for subsequent reviews of this authorisation: Only complete

this box if review dates after the first reviews are known. If not or inappropriate to set additional review dates then leave blank.				
Name (Print)		**Position**		
Signature		**Date and time**		
Authorising Officers should not normally be responsible for authorising operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially in the case of small organisations, or where it is necessary to act urgently or for security reasons.				
Expiry date and time				

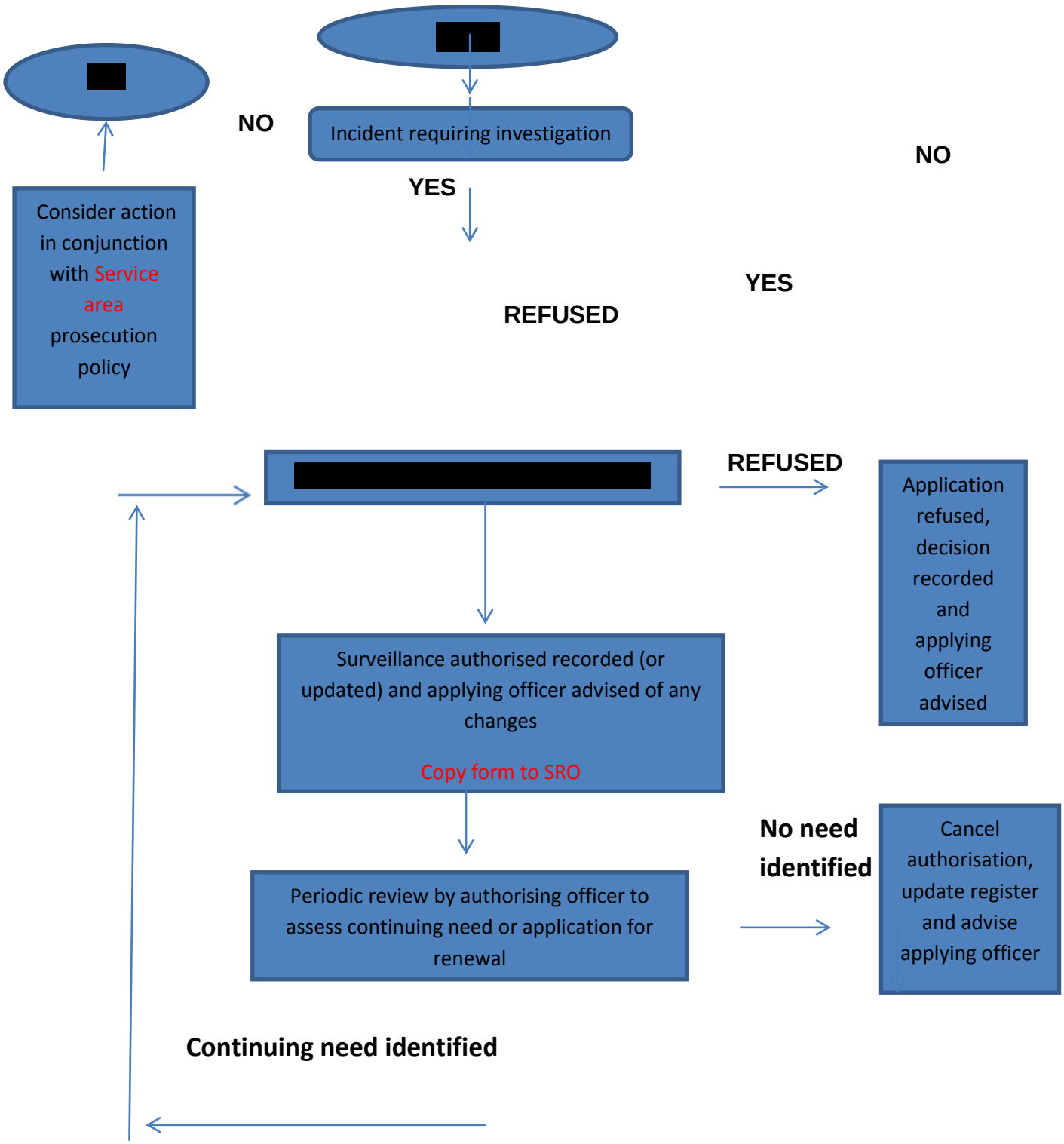
NOTE: Authorising Officers should notify the Senior Responsible Officer (Monitoring Officer) prior to completion of the form regardless of outcome

Once an authorisation has been granted, a copy of this form must be sent to the Senior Responsible Officer (Monitoring Officer).

Appendix C

NON - RIPA

Basic Lifecycle of a Directed Surveillance Authorisation



FLOWCHARTS