STOCKPORT
METROPOLITAN BOROUGH COUNCIL

CODE OF PRACTICE FOR CARRYING OUT SURVEILLANCE UNDER THE REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) AND INVESTIGATORY POWERS ACT 2016 (IPA)

Strategic Head of Service & Monitoring Officer
(Legal and Democratic Governance)
Stockport Metropolitan Borough Council
Town Hall
Edward Street
Stockport
SK1 3XE

Applications for and authorisation of surveillance & use of Covert Human Intelligence Sources

This document sets out the requirements for obtaining authorisation under RIPA and the IPA; the persons able to grant authorisation; circumstances when authorisation will be required; and the storage and maintenance of records of authorisation and the forms which Stockport Metropolitan Borough Council use.

Revision history:

v.1	**March 2004**	**RJ**
v.2	**July 2006**	**RJ**
v.3	**September 2007**	**CN**
v.4	**December 2009**	**CN**
v.5	**May 2010**	**CN**
v.6	**April 2013**	**SO**
v.7	**July 2013**	**SO**
v.8	**May 2016**	**JM**
v.9	**December 2016**	**JM**
v.10	**October 2019**	**MD**
v.11	**November 2020**	**MD**
v.12	**December 2022**	**MD**

Table of Contents

STOCKPORT METROPLITAN BOROUGH COUNCIL

Code of Practice for the carrying out of surveillance and the use of Covert Human Intelligence Sources under the Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act 2016 (IPA)

1 General Introduction

On the 2nd October 2000 the Human Rights Act 1998 (HRA) came into to full force, making it unlawful for a local authority to breach any article of the European Convention on Human Rights (ECHR). Any such breach will be dealt with by the UK courts directly rather than the lengthy process of using the European Court of Justice.

Article 8 of the ECHR states:

'*Everyone has the right to respect for his private and family life, his home and his correspondence*.'

Those who undertake covert surveillance on behalf of a public authority (whether employees or agents) are likely to breach a person's human rights unless the surveillance is authorised in accordance with the law and is necessary for the **purpose of prevention or detection of crime.** Authorisations on any other ground will not be in accordance with the Regulation of Investigatory Powers Act 2000 (RIPA). In the light of the implications of the HRA, RIPA passed through Parliament and came into force on 25th September 2000. The current codes of practice relating to covert surveillance were amended in 2018 (SI. 2014. Nos. 3103 and 3119).

Code of Practice SI. No. 3119 applies to covert surveillance or the use of Covert Human Intelligence Sources (CHIS). Definitions of all terminology follow. It should be emphasised that RIPA will only apply if the surveillance or use of the CHIS is from a covert source. Quite often, such surveillance activities will be done overtly therefore will fall outside RIPA.

Where there is interference with Article 8 of the ECHR, and where there is no other source of lawful authority for the interference, the consequences of not following the correct authorisation procedure set out under RIPA, the IPA or this Policy may result in the Council's actions being deemed unlawful by the Courts under Section 6 of the HRA or by the Investigatory Powers Tribunal, opening up the Council to claims for compensation and loss of reputation. Additionally, any information obtained that could be of help in a prosecution will be inadmissible.

2 Definitions

2.1 Surveillance

- Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- Recording anything monitored, observed or listened to in the course of surveillance.
- Surveillance by or with the assistance of a device.

2.1.1 Overt Surveillance

The majority of the Council's surveillance activity will be overt surveillance i.e. will be carried out openly. For example (i) where the Council performs regulatory checks on licensees to ensure they are complying with the terms of any licence granted; and (ii) where the Council advises a tenant that their activities will be monitored as a result of neighbour nuisance allegations **(iii) or where an officer uses body worn cameras and informs the individual that the camera will be switched on and recording will take place.** This type of overt surveillance is normal Council business and is not regulated by RIPA.

2.1.2 Covert Surveillance

This is where surveillance is carried out in a manner calculated to ensure that the person subject to the surveillance is unaware it is taking place.

Certain enforcement activities such as visits to premises for specific purposes are not surveillance. The purpose of the activity will determine whether it is covert. RIPA authorisation may be required where the activity is repeated for a particular purpose and could amount to systematic surveillance of an individual; if in doubt seek advice from the Legal Team.

Covert surveillance can be intrusive or directed. **The Council is not permitted to carry out covert intrusive surveillance**. Para 2.2 below explains when covert surveillance is intrusive and therefore not permitted. The Council is permitted to carry out covert directed surveillance subject to strict compliance with RIPA. Paragraph 2.3 below explains when covert surveillance is directed.

2.2 Covert Intrusive Surveillance

Covert intrusive surveillance takes place when covert surveillance is carried out in relation to anything taking place on residential premises or in a private vehicle and which involves the presence of an individual or surveillance device on the premises or in the vehicle, or which uses a device placed outside the premises or vehicle which consistently provides information of the same quality and detail as expected of a device placed inside.

Additionally, the Regulation of Investigatory Powers (Extension of Authorisations Provisions: Legal Consultations) Order 2010 states that covert

surveillance carried out in relation to anything taking place in certain specified premises is intrusive when they are being used for legal consultation.

2.3 Covert Directed Surveillance

This is surveillance that is:

- covert;
- not intrusive;
- for the purposes of a specific investigation or operation;
- likely to obtain private information[1] about a person (whether or not that person was the target of the investigation or operation); and
- not carried out as an immediate response to events or circumstances which could not have been foreseen prior to the surveillance taking place.

Directed surveillance involves the observation of a person or persons with the intention of gathering private information to produce a picture of a person's life, activities and associations. It does not include entry on or interference with property or wireless telegraphy but may include the use of photographic and video equipment (including the use of CCTV).

2.4 Confidential Information

A higher level of authorisation is required in relation to RIPA activity when the subject of the investigation might reasonably expect a high degree of privacy, or where "confidential information" might be obtained, prior to applying to the Magistrates Court for judicial approval. For the purpose of RIPA this includes:

- communications subject to legal privilege[2];
- communications between a member of parliament and another person on constituency matters;
- confidential personal information[3]; and
- confidential journalistic material[4]

---

[1] Private information includes any information relating to a person's private and family life, home and correspondence (whether at home, in a public place or in the work place).

[2] Legal privilege is defined in section 98 of the Police Act 1997 as:

- communications between a professional legal adviser and his client, or any person representing his client which are made in connection with the giving of legal advice to the client.
- communications between a professional legal adviser and his client or any person representing his client, or between a professional legal adviser or his client or any such representative and any other person which are made in connection with or in contemplation of legal proceedings and for the purposes of such proceedings.
- Items enclosed with or referred to in communications of the kind mentioned above and made in connection with the giving of legal advice, or in connection with or in contemplation of legal proceedings and for the purposes of such proceedings. Communications and items are not matters subject to legal privilege when they are in the possession of a person who is not entitled to possession of them, and communications and items held, or oral communications made, with the intention of furthering a criminal purpose are not matters subject to legal privilege.

If advice is required on this point, officers should contact the Head of Legal or the Democratic Services Legal Team.

[3] Confidential personal information is described at **paragraph 9.29 of the Home Office Covert Surveillance and Property Interference Revised Code of Practice.**

[4] Confidential journalistic material is described at **paragraph 9.38 of the Home Office Covert Surveillance and Property Interference Revised Code of Practice**.

The authorising officer and the person carrying out the surveillance must understand that such information is confidential and is subject to a stringent authorisation procedure. **Authorisation can only be granted by the Chief Executive or in their absence by an officer acting as Head of Paid Service.**

Any officer contemplating RIPA activity where the above circumstances may apply must seek advice from Legal Services prior to making any application.

2.5 Covert Human Intelligence Sources ("CHIS")

The Council is permitted to use a CHIS subject to strict compliance with RIPA.

A CHIS is a person who establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating:

(a) covertly using the relationship to obtain information or provide access to information to another person, or
(b) covertly disclosing information obtained by the use of the relationship or as a consequence of the existence of such a relationship.

A RIPA authorisation and order from a magistrate is required for the above activity and should be obtained whether the CHIS is a Council officer or another person who is asked to be a CHIS on the Council's behalf.

Authorisation for a CHIS can only be granted if it is for the purposes of "preventing or detecting crime or of preventing disorder."

Members of the public who volunteer information to the Council and those engaged by the Council to carry out test purchases in the ordinary course of business (i.e. they do not develop a relationship with the shop attendant and do not use covert recording devices) are not a CHIS and do not require RIPA authorisation. If the Council is using a team with surveillance equipment to support that operation, then this could then mean the volunteer is a CHIS and would require authorization.

In addition, by virtue of section 26(8) (c) of RIPA, it is possible that a person will become engaged in the conduct of a CHIS without the Council inducing, asking or assisting the person to engage in that conduct.

When an informant gives repeat information about a suspect or family, and it appears that this information is being obtained by the informant as part of a continued family or neighbourhood relationship, this could mean that the informant is in reality a CHIS.

The informant may be at risk of reprisals and the Council owes a duty of care to the informant if the information which has been passed on is ever used.

If any Council Officer believes that information they have been provided by an informant may result in the informant being engaged in the conduct of a CHIS, they should seek further legal guidance before acting on any of the information

provided.

If the Council then makes use of the information, and the informant is thereby put at risk, the Council may be in breach of its duty of care owed to the individual. It is recommended that legal advice is sought in any such circumstances.

The Home Office Covert Human Intelligence Sources Code of Practice can be found here.

2.6 Vulnerable Individuals / Juvenile CHIS

Additional requirements apply to the use of a vulnerable individual[5] or a person under the age of 18 as a CHIS. In both cases **authorisation for an application to the Magistrates Court can only be granted by the Chief Executive or in their absence by an officer acting as Head of Paid Service**. **Any officer contemplating the use of a juvenile or a vulnerable person as a CHIS must seek advice from the Legal Team prior to making the application.**

The use or conduct of a CHIS under 16 years of age **must not** be authorised to give information against their parents or any person who has parental responsibility for them.

In other cases, authorisations should not be granted unless the special provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 (as amended) are satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorization, which has now been extended to a maximum of 4 months.

2.7 Collateral Intrusion

Applications for authorisation should include an assessment of the risk of any collateral intrusion.

There will be a risk of collateral intrusion if the investigation is likely to interfere with the privacy of individuals who are not covered by the authorisation.

2.8 Authorising Officers

The Regulation of Investigatory Powers (Directe**d Surveillance and Covert Human** Intelligence Sources) Order 2010 No. 521 came into force on 6 April 2010 consolidates and amends previous orders and states that employees with the rank of Director, Head of Service, Service Manager or equivalent may be appointed as an Authorising Officer and authorise surveillance carried out under RIPA

Appendix 9 provides a list of Authorised Officers, by reference to their posts and names, who are able to assess surveillance requests on behalf of the Council

[5] A vulnerable individual is a person who by reason of mental disorder or vulnerability, other disability, age or illness, is or may be unable to take care of themselves or protect themselves against significant harm or exploitation.

and approve them for submission to a Magistrate for authorisation. Amendments to this list are to be agreed by the Head of Legal and Democratic Governance. Any amendments are to be recorded centrally by the RIPA Co-ordinator

Authorising Officers should not be responsible for assessing applications for their own activities i.e. those operations/investigations in which they are directly involved; however, it is recognised that this may sometimes be unavoidable, especially in the case of small organisations or where it is necessary to act urgently. If an Authorising Officer has to authorise a case in which he or she has been involved then this should be highlighted to the RIPA Co-ordinator where it will be brought to the attention of the Commissioner or Inspector during the next inspection.

If the person who has power to authorise the surveillance is not available, the authorisation must be given by a more senior officer (Reg 2 S.I.2000 3171).

Formal written authorisation is required to be an Authorised Officer and this will be reviewed on a case by case basis.

2.9 Private Information

This includes, 'in relation to a person', any information relating to his or her private or family life, as well as aspects of his or her business or professional life.

Viewing of open source material - Social Networking Sites**.** The Home Office Revised Code of Practice on Covert Surveillance and Property Interference, published in 2018, provides the following guidance in relation to online covert activity:

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

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

practice provide detail on where a CHIS authorisation may be available for online activity).

In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and a directed surveillance authorisation will not normally be available.

As set out below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information. Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

Whether a public authority interferes with a person's private life includes a consideration of the nature of the public authority's activity in relation to that information. Simple reconnaissance of such sites (i.e. preliminary examination with a view to establishing whether the site or its contents are of interest) is unlikely to interfere with a person's reasonably held expectation of privacy and therefore is not likely to require a directed surveillance authorisation. But where a public authority is systematically collecting and recording information about a particular person or group, a directed surveillance authorisation should be considered. These considerations apply regardless of when the information was shared online. See also paragraph 3.6 (of the Code).

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

Example 2: A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to

extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)

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

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

• Whether the investigation or research is directed towards an individual or organisation;

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

• Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;

• Whether the information obtained will be recorded and retained;

• Whether the information is likely to provide an observer with a pattern of lifestyle;

• Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;

• Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);

• Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

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

Example: Researchers within a public authority using automated monitoring tools to search for common terminology used online for illegal purposes will not normally require a directed surveillance authorisation. Similarly, general

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

There is a need to balance the level of interference with people's privacy against the seriousness of the problem being investigated. There should be the minimal amount of intrusion and a demonstration of the factors taken into consideration when deciding whether surveillance is necessary and proportionate.

Under no circumstances are personal devices or accounts to be used during the course of any investigation, reconnaissance or surveillance.

3 General Provisions About Authorisations

Surveillance will only be authorised where it is believed that the surveillance is **necessary** under the grounds set out below and is **proportionate** to what it seeks to achieve.

To protect privacy and comply with the HRA, all Council services will need to demonstrate that any intrusion into an individual's privacy is essential to an investigation.

Where surveillance is considered appropriate it will be necessary for it to be authorised before it can commence (except where covert surveillance is carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen).

Authorising Officers (see definition above at 2.8 and Appendix 9) will need to satisfy themselves that a defensible case can be made for surveillance activity before presenting the authorisation request to a Magistrate to obtain authorisation. Obtaining an authorisation will ensure that the action is carried out in accordance with law and subject to stringent safeguards against abuse. It will also make the action less vulnerable to challenge under the HRA.

4 Grounds for Authorisation of Directed Surveillance or use of a Covert Human Intelligence Source

Authorisation for both types of surveillance may be granted by a Magistrate where it is believe that the authorisation is **necessary** and the authorised surveillance is **proportionate** to that which is sought to be achieved. Please see paragraph 7.1 and 7.2 below for a further definition of *necessary* and *proportionate*.

The Regulation of Investigatory Powers (Directed Surveillance and Covert

Human Intelligence Sources) Order 2003 which came into force on the 5th January 2004 places restrictions on the grounds for authorisations under Section 28(3) and 29(3).

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012/1500 places further restrictions on the grounds for which authorisations under Section 28(3) may be obtained meaning that authorisation may only be obtained in relation to criminal behaviour which satisfies the 'Serious Crime Test' unless an exemption applies.

Certain offences relating to the sales of alcohol and tobacco are excluded from the serious crime test[6].

5 Serious Crime Test

Where local authorities wish to use RIPA to authorise Directed Surveillance, this must be confined to cases where the offence under investigation carries a custodial sentence of six months or more. This is called the 'Serious Crime Test'.

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 came into force on 1st November 2012.

A flowchart detailing the considerations of the Serious Crime test is attached at Appendix 10.

6 Additional Requirements for Authorisation of Covert Human Intelligence Sources Only

Covert human intelligence sources may only be authorised if the following additional arrangements are in place:

- There is an employee of the Council with day-to-day responsibility for dealing with the source and for the source's security and welfare. This person will adopt the role of 'CHIS Handler'
- There is a senior officer who has general oversight of the use made of the source. This person will adopt the role of 'CHIS Controller'
- An officer will be responsible for maintaining a record of the use made of the source.
- Those records will contain any matters specified by the Secretary of State - The Regulation of Investigatory Powers (Source Records) Regulations 2000 set out these matters.
- Records disclosing the identity of the source will not be made available to others except on a need to know basis.

7 What to take into account when authorising surveillance or the Acquisition of Communications Data

The application and authorisation request should explain why the investigation is

[6] Notable exemptions include offences under Section 146/147/147A of the Licensing Act 2003, or Section 7 of the Children and Young Persons Act 1993.

necessary i.e. why is it necessary to take **this particular course of action** in order to prevent and detect crime?

Once satisfied that the authorisation is necessary, the Authorising Officer/Designated Person will then need to be satisfied that the proposed surveillance or acquisition is proportionate to the end that it is seeking to achieve. This involves balancing the intrusiveness of the activity on the subject and others who may be affected by the surveillance against the expected outcomes of the surveillance e.g. is a significant crime suspected? Is this affecting the local community? It will not be sufficient to simply assert that the proposed surveillance **is** proportionate without stating **why** it is. When considering proportionality, applicants and Authorising Officers must consider any methods already used to try to obtain the information and the outcome of those when explaining why they think that surveillance is a proportionate response, given that it will intrude into other people's privacy. The Authorising Officer must be able to produce evidence to show that the relevant issues have been considered for monitoring purposes e.g. a note of the documents and information available to the Officer at the time the authorisation is given can be included on the authorisation request form.

Authorising Officers must be satisfied that a full and detailed account of the surveillance operation is given on the authorisation request form. The Authorising Officer needs to be satisfied that they are fully aware of the nature of the surveillance including the exact location (plans should be provided), how this will be carried out and the identities of the Officers who will carry out the surveillance.

Particular consideration should be given to collateral intrusion into or interference with the privacy of persons other than the subject(s) of surveillance. This will be taken into account by the Authorising Officer, particularly when considering the proportionality of the surveillance.

Any Authorising Officer will also need to be aware of particular sensitivities in the local community where the surveillance is taking place or of similar activities being undertaken by other public authorities which could impact on the deployment of surveillance. In this regard, it may be necessary to consult local police or other agencies as appropriate where the Authorising Officer considers that conflicts might arise.

8 Magistrates Approval

Chapter 2 of Part 2 of the Protection of Freedoms Act 2012 (sections 37 and 38) amends RIPA so that it will now be required for local authorities to obtain the approval of a Magistrate for the use of any available RIPA techniques.

Magistrates approval is also required on the renewal of any such applications.

The new provisions give the Magistrate the power, when refusing an authorisation, to quash that authorisation.

It is therefore essential that, following approval from the relevant RIPA Authorising Officer, the Investigating Officer will present the authorisation to the Magistrate and obtain Magistrate Approval.

A flowchart detailing the RIPA authorisation process is attached at Appendix 11.

The Authorising Officer should use the relevant judicial approval forms when seeking Magistrate approval.

9 What Happens if the Surveillance has Unexpected Results?

Those carrying out the covert surveillance should inform the Authorising Officer if the operation/investigation unexpectedly interferes with the privacy of individuals who are not either the original subjects of the investigation or covered by the authorisation in some other way. In some cases the original authorisation may not be sufficient and consideration should be given to whether a separate authorisation is required.

10 Collaborative Working

The Council will often work with partners and other organisations e.g. joint operations between Trading Standards and the police. In such cases there may be confusion around who should obtain an authorisation under RIPA.

If a Council service is acting on behalf of another organisation e.g. Trading Standards is acting on behalf of the Police rather than carrying out its own independent investigation, the Police should provide the RIPA authorisation. In such cases, the application and authorisation will be completed by the Police and not the Council.

If the Council is carrying out its own investigation but it is clear from the outset that operational support will be required as part of the investigation from another organisation e.g. the police, this should be stated in the authorisation.

Where joint operations are carried out, only one authorisation is required. This minimises the amount of paperwork required and avoids duplication; however in cases where each party to the investigation completes an authorisation, the lawfulness of the activities will not be affected.

11 Duration of Authorisations

11.1. Directed Surveillance

A directed surveillance authorisation lasts for **three months** unless it is cancelled or renewed.

11.2. Review

Regular reviews of authorisations should be undertaken to assess the need for surveillance to continue. It is the responsibility of the Authorising Officer to set the review date when preparing the authorisation. The review date should be no more than one month from the date of the authorisation being approved in all cases. The results of any review should be kept on the Central Record

maintained by the RIPA Co- ordinator in Legal Services. There will be a greater need to review authorisations where the surveillance leads to confidential information being obtained or to collateral intrusion. The forms attached at Appendix 2 should be used for reviews.

Where an operation is expected to be completed quickly, the Authorising Officer should ensure that the authorisation is reviewed within a short time period to ascertain whether the surveillance is still necessary and proportionate. Review dates should not be set further than one month in advance. If the surveillance is no longer necessary or proportionate it should be cancelled using the appropriate form immediately. If further surveillance is necessary then a written application to renew the authority must be made using the appropriate form (see Appendix 4). A renewal of a directed surveillance lasts for a period of three months.

11.3. For the use of CHIS:

A CHIS authorisation lasts for 12 months unless cancelled or renewed. A juvenile CHIS authorisation lasts for four months unless cancelled or renewed. All authorisations must be cancelled when they are no longer necessary or proportionate.

When an Authority is considering the deployment of a CHIS who is;

- A Vulnerable Individual;
- A Juveniles or;
- Is likely to obtain confidential information

a higher level of authorisation is required. This authorisation must come from the Chief Executive.

The Chief Executive must be satisfied that the deployment of the CHIS is:

- Necessary on one of the grounds outlined in Section 29(3) of the RIPA 2000 Act;
- Proportionate to what is sought to be achieved; and
- The Special duties outlined in S29(5) of the 2000 Act are followed.

Following this authorisation being obtained, it is also necessary to obtain the Magistrates approval before any such surveillance commences or is renewed.

11.4. Review

Regular reviews of authorisations should be undertaken as with directed surveillance and the guidance given above on reviews applies equally to the use of CHIS.

The Authorising Officer should review the authorisation, taking into account whether the authorisation is still necessary and proportionate based on the operational requirements. The results of any review should be kept on a Central Record in Legal Services. There will be a greater requirement to review

authorisations where the surveillance leads to confidential information being obtained or to collateral intrusion. The forms attached at Appendix 6 should be used for such reviews.

11.5. Renewal

If further surveillance is necessary then a written application to renew the authorisation must be made using the appropriate form at Appendix 8. A renewal of a CHIS authorisation lasts for a further 12 month period.

12 Cancellation of Authorisations

The Authorising Officer who granted or last renewed the authorisation must cancel it when they are satisfied that the directed or CHIS surveillance no longer meets the criteria for authorisation. Cancellation should be recorded on the appropriate form at Appendix 7. All authorisations should be cancelled as soon as they are no longer required and should not be left to expire.

13 Records and Documentation

Applications, reviews, renewals and cancellations should be retained and a record kept of all such authorisations. These records will be confidential and should be retained for a period of at least five years from the end of the authorisation. The original documentation must be forwarded in an email or envelope marked ‘Private and Confidential’ to the appropriate Officer within Legal Services who has management of the Central Record of authorisations. This is currently Michelle Dodds (RIPA Co-ordinator). From time to time this Officer may change and subsequent changes will be notified to the Authorising Officers.

All documentation relating to an authorisation which forms part of the Central Record will be securely destroyed after a period of five years from the date of cancellation or expiry unless the investigating department can demonstrate it is needed for a longer period. This means in practice that applications, renewals, cancellations, reviews and copies of notices and any hard or electronic copies of communications relating to these must be permanently deleted/destroyed by any person who has created, sent, received or held them. The RIPA Co-ordinator will notify the applicant and Authorising Officer of the date of destruction and send a reminder when this is due and seek confirmation of the deletion/destruction. It will be the responsibility of the Authorising Officer to check and confirm that all records and documentation have been destroyed.

Where it is believed that the records could be relevant to pending or future court proceedings they should be retained for a suitable further period, subject to any subsequent review. Investigating departments must ensure they securely destroy any local copies of documentation in line with this practice.

14 Acquisition and Disclosure of Communications Data

Communication Service Providers (CSPs) are organisations that are involved in the provision, delivery and maintenance of communications such as postal,

telecommunication and internet service providers but also, for example, hotel or library staff involved in providing and maintaining e-mail access to customers. The Council must obtain communications data from CSPs in strict compliance with RIPA.

Communications Data ('CD') is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). Local Authorities are not permitted to intercept the content of any person's communications.

Part 3 of the Investigatory Powers Act 2016 (IPA) replaced part 1 chapter 2 of RIPA in relation to the acquisition of communications data (CD) and puts local authorities on the same standing as the police and law enforcement agencies. Previously local authorities have been limited to obtaining subscriber details (known now as "entity" data) such as the registered user of a telephone number or email address. Under the IPA, local authorities can now also obtain details of in and out call data, and cell site location. This information identifies who a criminal suspect is in communication with and whereabouts the suspect was when they made or received a call, or the location from which they were using an Internet service. This additional data is defined as "events" data.

A new threshold for which CD "events" data can be sought has been introduced under the IPA as "applicable crime". Defined in section 86(2A) of the Act this means: an offence for which an adult is capable of being sentenced to one year or more in prison; any offence involving violence, resulting in substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal; any offence committed by a body corporate; any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy. Further guidance can be found in paragraphs 3.3 to 3.13 of CD Code of Practice.

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/757850/Communications_Data_Code_of_Practice.pdf

Finally, the IPA has also removed the necessity for local authorities to seek the endorsement of a Justice of the Peace when seeking to acquire CD. All such applications must now be processed through the National Anti-Fraud Network (NAFN) and will be considered for approval by the independent Office of Communication Data Authorisation (OCDA). The transfer of applications between local authorities, NAFN and OCDA is all conducted electronically and will therefore reduce what can be a protracted process of securing an appearance before a Magistrate or District Judge (see local authority procedures set out in paragraphs 8.1 to 8.7 of the CD Code of Practice).

14.1 Additional Requirements for Authorisation of Acquisitions and Disclosure of Communications Data

The rules on the granting of authorisations for the acquisition of communications

data are slightly different from directed surveillance and CHIS authorisations and involve three roles within the Council. The roles are:

- Applicant Officer
- Designated Senior Officer (DSO)
- Single Point of Contact

Applicant

This is the officer involved in conducting an investigation or operation who makes an application in writing for the acquisition of communications data. The application form must:

- set out the legislation under which the operation or investigation is being conducted. This must be a statutory function of the Council for the prevention or detection of crime or preventing disorder.
- describe the communications data required i.e. the telephone number, email address, the specific date or period of the data and the type of data required. If the data will or may be generated in the future, the future period is restricted to no more than one month from the date on which the authorisation is granted.
- explain why the conduct is necessary and proportionate.
- consider and describe any meaningful collateral intrusion. For example, where access is for 'outgoing calls' from a 'home telephone' collateral intrusion may be applicable to calls made by family members who are outside the scope of the investigation. The applicant therefore needs to consider what the impact is on third parties and try to minimise it.

Designated Senior Officer

This is the person who makes the application. A Designated Senior Officer's role is the same as an authorising officer's role in relation to directed surveillance and CHIS authorisations. The DSO assesses the necessity and proportionality for any conduct to obtain communications data taking account of any advice provided by the single point of contact (SPoC).

A list of DSO's is available on the Council's intranet. Any requests for amendments to the lists must be made in writing and sent to the Head of Legal. Section73 of the IPA 2016 prescribes the rank or position of such officers as being a "Director, Head of Service, Service Manager or equivalent")

The Assistant Director – Legal & Democratic Governance designates which officers can be DSO's. Only these officers can authorise the disclosure of communications data.

Single Point of Contact (SPoC)

The accredited SPoCs at NAFN scrutinise the applications independently, and provide advice to applicant officers and DSO's and will be responsible for submitting the application to the OCDA on behalf of the Council.

15 Criminal Investigations

All observations should be recorded in accordance with recognised good practice and in compliance with the Criminal Procedure and Investigations Act 1996 (CPIA). Failure to comply with the requirements of CPIA or to ensure that evidence is recorded and retained properly will raise questions about the admissibility of the evidence and whether an abuse of process has occurred. Only surveillance-trained staff should undertake covert surveillance.

16 CCTV

The installation and use of unconcealed CCTV cameras for the purpose of generally observing activity in a particular area is not surveillance requiring RIPA authorisation. However, there are specific provisions regulating the use of CCTV cameras in public places and buildings and the Council has drawn up a Corporate CCTV Policy which officers must comply with and which can be found here on the Council's intranet. However if CCTV cameras are being used in such a way that the definition of covert directed surveillance is satisfied, RIPA authorisation should be obtained.

For instance the use of town centre CCTV systems to identify those responsible for a criminal act immediately after it happens will not require RIPA authorisation. However, the use of the same CCTV system to conduct planned surveillance of an individual and record his movements is likely to require authorisation.

Protocols should be agreed with any external agencies requesting use of the Council's CCTV system. The protocols should ensure that the Council is satisfied that authorisations have been validly granted prior to agreeing that the CCTV system may be used for directed surveillance.

17 Roles and Responsibilities

The Investigatory Powers Commissioners Office (IPCO) has a duty to keep the exercise and performance of the Council's surveillance powers under review. IPCO will regularly inspect the Council.

The Assistant Director – Legal & Democratic Governance is required by law to ensure that the Council does not act unlawfully.

To ensure that proper monitoring of surveillance activity can be carried out with minimum disruption; records will be retained, maintained and monitored by the RIPA Co-ordinator on behalf of Head of Legal and Democratic Services.

The Assistant Director – Legal & Democratic Governance is the Senior Responsible Officer (SRO) and RIPA Monitoring Officer. The SRO has overall responsibility for ensuring that the Council complies with RIPA. The SRO/RIPA Monitoring Officer will inspect authorisations on a quarterly basis, deliver training to employees and participate in IPCO inspections, as well as delivering reports to elected members on the Council's use of RIPA.

Day-to-day responsibility for RIPA compliance is delegated to the RIPA Co-ordinator (contact Michelle Dodds – RIPA Co-ordinator: michelle.dodds@stockport.gov.uk; Corporate Support Services Legal & Democratic Services Room 326 Town Hall Stockport SK1 3XE 0161 474 3257. The RIPA Co-ordinator maintains the Central Record and the RIPA intranet site, carries out quality assurance checks on all authorisations submitted, delivers training, provides day-to-day advice on surveillance issues and produces reports to be delivered to elected members.

Records kept by the RIPA Co-ordinator will be used to:

- remind Authorising Officers of the expiry of authorisations
- check that surveillance does not continue beyond the authorised period
- remind Authorising Officers to regularly review current authorisations
- remind Authorising Officers and applicants to consider the destruction of the results of surveillance operations and associated paperwork in line with retention and destruction guidelines
- at the fifth anniversary of each authorisation, remind Authorising Officers that the forms of authorisation, renewal or cancellation held locally and in the Central Record maintained by the RIPA Co-ordinator are due to be destroyed unless there is a reason they should be retained for longer.
- receive and investigate complaints by members of the public who reasonably believe that they have been adversely affected by surveillance activities carried out by the Council
- commission and provide training in the law relating to surveillance for Officers who are applying for and authorising surveillance.

18 Reporting to elected members

In line with the Home Office Code of Practice 'Covert Surveillance and Property Interference' current version August 2018 (section 4.47), this Stockport Council Code of Practice will be approved by the appropriate the Corporate, Resource Management and Governance Scrutiny Committee on an annual basis to ensure that it remains fit-for-purpose and to ensure it is using its powers in line with the Council's Code of Practice; however elected members should not be involved in making decisions in relation to specific operations and authorisations.

19 Complaints

Any person who reasonably believes they have been adversely affected by surveillance activity carried out by or on behalf of the Council may complain to the Assistant Director – Legal & Democratic Governance & Monitoring Officer who will investigate the complaint.

Assistant Director – Legal & Democratic Governance & Monitoring Officer
Town Hall
Stockport
Cheshire

SK1 3XE

Such a person may also complain to the Investigatory Powers Tribunal at:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

20 LIST OF APPENDICES

APPENDIX 1 - Application for Authorisation of Directed Surveillance

APPENDIX 2 - Review of Directed Surveillance Authorisation

APPENDIX 3 - Cancellation of Directed Surveillance Authorisation

APPENDIX 4 - Renewal of Directed Surveillance Authorisation

APPENDIX 5 - Application for Authorisation of a Covert Human Intelligence Source

APPENDIX 6 - Review of Covert Human Intelligence Source Authorisation

APPENDIX 7 - Cancellation of Covert Human Intelligence Source Authorisation

APPENDIX 8 - Renewal of Covert Human Intelligence Source Authorisation

APPENDIX 9 - List of Authorising Officers (appended)

APPENDIX 10 – Serious Crime Test Flowchart (appended)

APPENDIX 11 – RIPA Authorisation Flowchart (appended)

APPENDIX 12 – Judicial Application Form

APPENDIX 13 - Magistrates Approval Process (appended)

Stockport Council Authorising Officers – Regulation of Investigatory Powers Act 2000 (RIPA) and Investigatory Powers Act 2016 (IPA)

Chief Executive

Caroline Simpson
(Applications for surveillance which is likely to obtain confidential information/involve a juvenile or vulnerable person)

PLACE Directorate

Ian O'Donnell	Head of Public Protection
Mark Glynn	Director of Place Management
Emma Stubbs	Strategic Head of Neighbourhoods

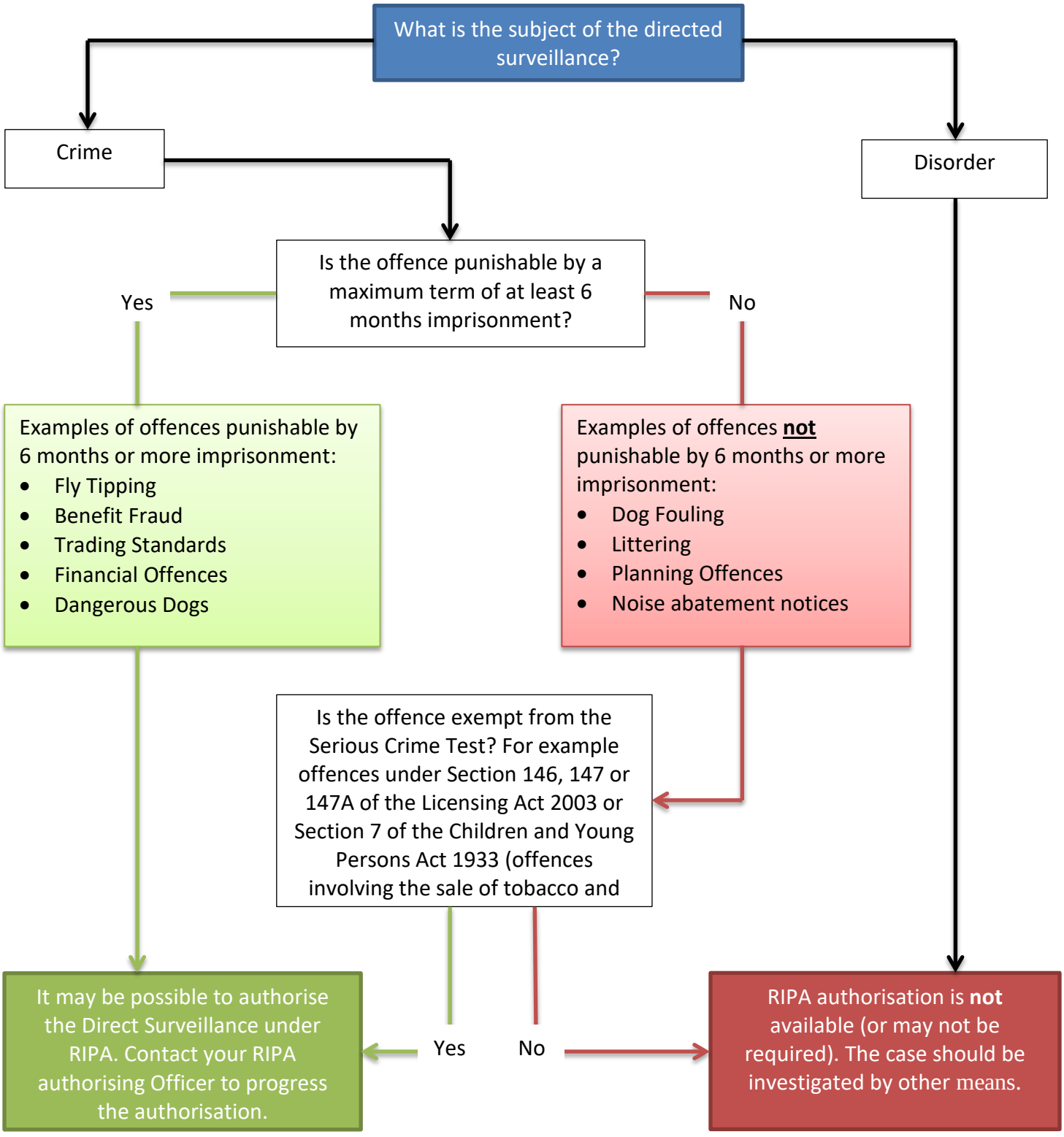
Designated Persons for Telecommunications

Ian O'Donnell	Head of Public Protection

Annex 2: RIPA - Serious Crime Test

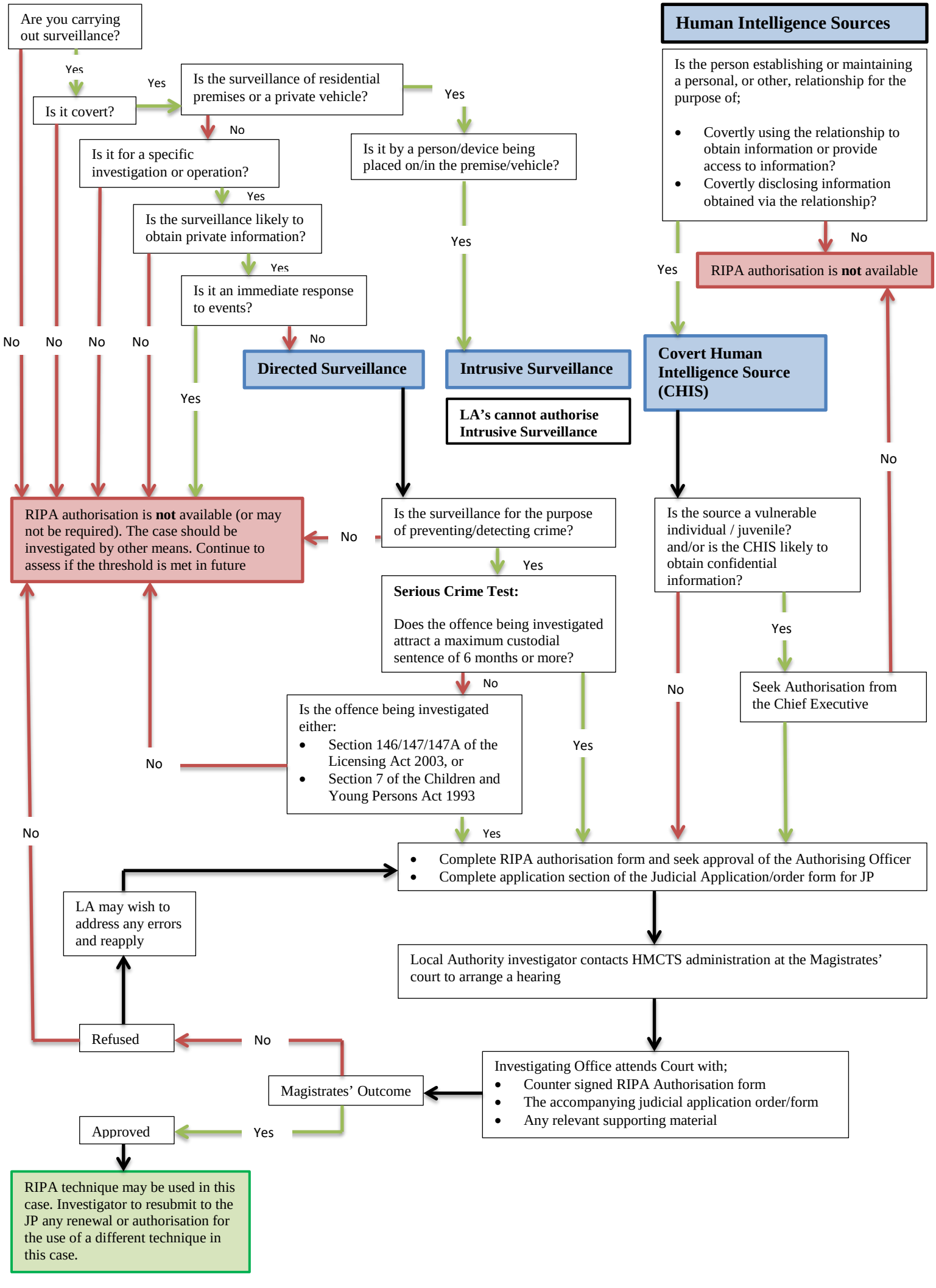
The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources)(Amendment) Order 2012, SI 2012/1500 governs the conditions in which Local Authorities can obtain RIPA authorisations for undertaking Directed Surveillance.

The Flowchart below outlines the criteria which must be met to satisfy the 'Serious Crime Test' which is required to be passed prior to any Directed Surveillance being authorised.



Annex 1: RIPA Authorisation Flowchart

Appendix 11



APPENDIX 13

Magistrates Approval Process

1. The first stage will be to apply for an internal authorisation in the usual way. Once it has been granted, the Local Authority will need to contact the local Magistrates Court 1-2 days before, to arrange a hearing.
2. The hearing is a 'legal proceeding' and therefore local authority officers need to be formally designated to appear, be sworn in and present evidence or provide information as required by the Justice of Peace (JP).
3. The Investigating Officer will attend the court and present themselves to the enquiries desk. Prior to the hearing the delegate will be seen by a legally qualified person who will go over the application in detail to seek out any obvious issues, this is known as the gateway check.
4. The local authority will provide the JP with a copy of the original RIPA authorisation. This forms the basis of the application to the JP and should contain all information that is relied upon. In addition, the local authority will provide the JP with two copies of a partially completed judicial application form,
5. The hearing will be in private and heard by a single JP who will read and consider the RIPA authorisation or notice and the judicial application/order form. He/she may have questions to clarify points or require additional reassurance on particular matters. The forms and supporting papers must by themselves make the case. It is not sufficient for the local authority to provide oral evidence where this is not reflected or supported in the papers provided.
6. The JP will consider whether he or she is satisfied that at the time the authorisation was granted or renewed or the notice was given or renewed, there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate. He/She will also consider whether there continues to be reasonable grounds. In addition they must be satisfied that the person who granted the authorisation or gave the notice was an appropriate designated person within the local authority and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met (see below).
7. The order section of the above mentioned form will be completed by the JP and will be the official record of his/her decision. The local authority will need to retain a copy of the form after it has been signed by the JP.

The Magistrates Approval Process

Local authority investigator wants to use a RIPA technique (directed surveillance or covert human intelligence sources).

Does investigator intend to use directed surveillance?

Y

N

Is the local authority investigating an offence and does that offence attract a maximum custodial sentence of 6 month or more?

N

Y

Is the offence being investigated either:
- Section 146/147/147A of the Licensing Act 2003, or
- Section 7 of the Children and Young Persons Act 1993.

N

Y

Investigator may **not** conduct directed surveillance. The case should be investigated by other means. Continue to assess if threshold is met **if** further offences come to light as the case progresses.

- Complete RIPA authorisation form, and seek approval of authorising officer as per current arrangements.
- Complete application part of the judicial application/order form for JP.

Within Office Hours
Local authority investigator to contact Her Majesty's Courts & Tribunals Service (HMCTS) administration at the magistrates' court to arrange a hearing.

Attend court with:
- counter-signed RIPA authorisation;
- the accompanying judicial application form;
- any other relevant reference or supporting material.

Outcome

Refuse to approve the grant or renewal and quash the authorisation.

This may be appropriate if the JP considers that an application is fundamentally flawed. The local authority must be given at least 2 business days in which to make representations before the authorisation is quashed. In these circumstances a local authority cannot use the technique and will need to seek further authorisation internally before reapplying.

Refuse to approve the grant renewal of an authorisation.

The grant or renewal of the RIPA authorisation will not take effect and the local authority may **not** use the cover t technique. Local authority may wish to address, for example, a technical error and reapply.

Approve the grant or renewal of an authorisation.

Technique may be used in this case. Investigator to resubmit to the JP any renewal or authorisation for the use of a different technique in this case.

Outside usual office hours:

A JP may consider an authorisation out of hours in **exceptional** circumstances. If the authorisation is urgent and cannot be handled the next working day then you should:
- Phone the court's out of hours HMCTS legal staff contact. You will be asked about the basic facts and urgency of the authorisation. If the police are involved in the investigation you will need to address why they cannot make a RIPA authorisation.
- If urgency is agreed, then arrangements will be made for a suitable JP to consider the application. You will be told where to attend and give evidence.
- Attend hearing as directed with two copies of both countersigned RIPA authorisation form and the accompanying judicial application form.

Obtain signed order and retain original RIPA authorisation.

For further information, please refer to the Home Office Guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance.