Bolsover District Council

RIPA Policy

September 2024

Equalities Statement

Bolsover District Council is committed to equalities as an employer and when delivering the services it provides to all sections of the community.

The Council believes that no person should be treated unfairly and is committed to eliminating all forms of discrimination, advancing equality and fostering good relations between all groups in society.

Access for All statement

You can request this document or information in another format such as large print or **language** or contact us by:

- **Phone:** 01246 242424
- **Email:** enquiries@bolsover.gov.uk
- **BSL Video Call:** A three-way video call with us and a BSL interpreter. It is free to call Bolsover District Council with Sign Solutions, you just need WiFi or mobile data to make the video call, or call into one of our Contact Centres.
- Call with Relay UK - a free phone service provided by BT for anyone who has difficulty hearing or speaking. It's a way to have a real-time conversation with us by text.
- **Visiting** one of our offices at Clowne, Bolsover, Shirebrook and South Normanton

Policy Details	Comments / Confirmation (To be updated as the document progresses)
Policy title	RIPA Corporate Policy and Procedures
Current status – i.e. first draft, version 2 or final version	Draft (2024 Review)
Policy author	
Location of policy – i.e. L-drive, shared drive	S Drive
Member route for approval	Standards Committee
Cabinet Member (if applicable)	
Equality Impact Assessment approval date	July 2017
Partnership involvement (if applicable)	N/A
Final policy approval route i.e. Executive/ Council /Planning Committee	Standards Committee
Date policy approved	
Date policy due for review (maximum three years)	xx 2027
Date policy forwarded to Strategy and Performance (to include on Intranet and Internet if applicable to the public)	

Contents

Abbreviations

CCTV	Closed Circuit Television
Council	Bolsover District Council
CHIS	Covert Human Intelligence Source
DPA	Data Protection Act 2018
ECHR	European Convention for the Protection oh Human Rights
HRA	Human Rights Act 1998
IPA	Investigatory Powers Act 2016
IPCO	Investigatory Powers Commissioners Office
JP	Justice of the Peace / Magistrate
NAFN	National Anti-Fraud Network
POFA	Protection of Freedoms Act 2012
RIPA	Regulation of Investigatory Powers Act 2000
SPOC's	Single Points of Contact
SRO	Senior Responsible Officer (Monitoring Officer)

SECTION 1 - POLICY STATEMENT

Introduction

1. This Policy document is based upon the requirements of the Regulation of Investigatory Powers Act 2000, the national Code of Practice issued by the Home Office and Investigatory Powers Commissioner's Office. Links to the Home Office Guidance and Codes of Practice can be found here https://www.gov.uk/government/collections/ripa-codes

2. In limited circumstances the Council may wish to use surveillance techniques for the purpose of enforcing this Policy or other of its statutory functions. The requirements of RIPA and the IPA are most likely to apply to those sections of the Council with enforcement / investigatory functions.

3. RIPA is concerned with the regulation of surveillance and other intelligence gathering by public authorities in the conduct of legitimate business. IPA sets out the extent to which certain investigatory powers may be used to interfere with privacy.

4. RIPA sets out procedures that must be followed to ensure investigatory activity is lawful. Where properly authorised under RIPA the activity will be a justifiable interference with an individual's rights under the ECHR. If the interference is not properly authorised an action for breach of the HRA could be taken against the Council, a complaint of maladministration made to the Local Government

Ombudsman or a complaint made to the Investigatory Powers Tribunal. In addition, if the procedures are not followed any evidence collected may be disallowed by the courts.

5. IPA sets our procedures for the interception of communications, equipment interference and the acquisition and retention of communications data.

6. The aims of RIPA and IPA are to provide a balance between preserving people's right to privacy and enabling enforcement agencies to gather evidence for effective enforcement action. RIPA provides a statutory framework for the use of certain types of covert surveillance, IPA provides the statutory framework for the lawful interception and use of communications data.

7. Any potential use of RIPA / IPA should be referred to the Monitoring Officer for preliminary advice at the earliest possible opportunity on 01246 242472. In the Monitoring Officer's absence, advice should be sought from Legal Services Team Manager /Deputy Monitoring Officer on 01246 242 507.

PART 1 – RIPA

What RIPA does and does not do

1. RIPA **does**:-
   - require prior authorisation and judicial approval of directed surveillance;
   - prohibit the Council from carrying out intrusive surveillance;
   - require authorisation of the conduct and use of CHIS;
   - require safeguards for the conduct of the use of a CHIS.

2. RIPA **does not**:-
   - make unlawful conduct which is otherwise lawful;
   - prejudice or disapply any existing power available to the Council to obtain information by any means not involving conduct that may be authorised under RIPA. For example, it does not affect the Council's current powers to obtain information from the DVLA as to the owner of a vehicle or to obtain information from the Land Registry as to the owner of a property;

3. RIPA only applies to the Council's core functions – i.e. its statutory duties, and not staffing issues or contractual disputes.

Procedure

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

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

a. Human Rights Act 1998
b. Regulation of Investigatory Powers Act 2000
c. Protection of Freedoms Act 2012
d. Data Protection Act 2018

6. The Council will also have due regard to all official guidance and codes of practice particularly those issued by the Home Office, the Investigatory Powers Commissioner's Office, the Surveillance Camera Commissioner and the Information Commissioner.

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

• Covert surveillance will only be undertaken where it is absolutely necessary to achieve the desired aims.

• Covert surveillance will only be undertaken where it is proportionate to do so and in a manner that it is proportionate.

• Adequate regard shall be had to the rights and freedoms of those who are not the target of the covert surveillance

• All authorisations to carry out covert surveillance shall be granted by appropriately trained and designated authorising officers. A list of those authorising officers who have been nominated by their Directorate and have undertaken appropriate training is held by the SRO.

• Covert surveillance which is regulated by RIPA shall only be undertaken after obtaining judicial approval.

• The operation of this Policy will be overseen by the SRO, whose role is described later in this document.

Training

8. The SRO / Monitoring Officer will arrange regular training on RIPA. All authorising officers, designated persons and investigating officers should attend at least one session every two years and further sessions as and when required.

9. All Council officers undertaking and authorising covert surveillance shall be appropriately trained to ensure that they understand their legal and moral obligations.

10. Training can be arranged on request and requests should be made to the Monitoring Officer. In particular training should be requested for new starters within the Council who may be involved in relevant activities.

SECTION 2 - SURVEILLANCE

Types of Surveillance

1. Surveillance can be **overt** or **covert** and includes:-
    - 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; and
    - Surveillance by or with the assistance of a device

2. Indicators of whether investigatory activity will amount to surveillance include the formality and duration of the activity and the nature of what is being observed.

Overt Surveillance

3. 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. **This type of overt surveillance is normal Council business and does not require authorisation under RIPA.**

4. If Surveillance is being done openly, without making any attempt to conceal it or a warning letter is served on the target before the Surveillance is to be done, then it will be overt.

Covert Surveillance

5. 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. Covert surveillance can be intrusive or directed. The Council is not permitted to carry out covert intrusive surveillance. Paragraph 8 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 9 below explains when covert surveillance is directed.

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

7. The purpose of this part of the procedure is to help you decide what type of surveillance you are doing and whether it is therefore regulated by Part 2.

Covert Intrusive Surveillance

8. 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. **The Council is not permitted to carry out this type of surveillance.** (see **Flowchart 1)**

Covert Directed Surveillance

9. This is surveillance that is:-
    - Covert;
    - Not intrusive;
    - For the purposes of a specific investigation or operation;
    - Likely to obtain private information* 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.

    * Private information includes any information relating to a person's private and family life including professional and business relationships, home and correspondence (whether at home, in a public place or in the work place).

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

11. To help in deciding whether surveillance is Directed Surveillance please refer to **Flowchart 2**

12. Key points to note in relation to Directed Surveillance:-

    • General observations do not constitute Directed Surveillance. The Covert Surveillance Code (para 3.33) states:

    "The general observation duties of many law enforcement officers and other public authorities do not require authorisation under the 2000 Act, whether covert or overt. Such general observation duties frequently form part of the legislative functions of public authorities, as opposed to the pre-planned surveillance of a specific person or group of people."

    • Surveillance is only Directed if it is covert. RIPA section 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;"

13. Where covert Surveillance needs to be done in an emergency and without time to authorise the activity (or where no Authorising Officer is immediately available) the surveillance can still be done. It will not constitute Directed Surveillance. The Covert Surveillance Code (para 3.32) states:

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

Directed Surveillance and Social Media

14. The use of the internet may be required to gather information prior to and/or during an investigation, which may amount to Directed Surveillance. Although information that individuals make publicly available on the internet would not normally be classed as 'private information'.

15. The revised Code of Practice for Covert Surveillance and Property Interference clarifies the position on the use of social media for surveillance and states at paras 3.10 to 3.17

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

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

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

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

3.13 As set out in paragraph 3.14 below, depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether a user of a website or social media platform has sought to protect such information by restricting its access by activating privacy settings.

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

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

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

1. *Whether the investigation or research is directed towards an individual or organisation;*
2. *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);*
3. *Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;*
4. *Whether the information obtained will be recorded and retained;*
5. *Whether the information is likely to provide an observer with a pattern of lifestyle;*
6. *Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;*
7. *Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);*
8. *Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.*

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

16. The Council does not ordinarily permit the use of false personas to obtain information.

17. Officers should not make repeated visits to the same open source social media site as part of an investigation without first speaking with the SRO or Legal Services to ensure their actions are lawful.

CCTV

18. 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. There are specific provisions relating the use of CCTV cameras in public places and buildings. 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.

19. For example 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 their movements is likely to require authorisation.

20. Protocols should be agreed with any external agencies requesting the 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.

21. CCTV systems cannot be used without prior production of an authorisation and such authorisations must be retained.

SECTION 3 - COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

1. 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.

2. To help in deciding whether surveillance involves a CHIS please refer to **Flowchart 3**

3. Key points to note in relation to CHIS'

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

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

   • Merely giving a complainant a diary sheet to note comings and goings will not make that person a CHIS. There must be covert use of the relationship to provide access to, or to disclose information covertly for someone to be a CHIS. Other authorisations under RIPA, for example, a directed surveillance authorisation, may need to be considered where the activity is likely to result in the public authority obtaining information relating to a person's private or family life.

   • A test purchaser may not always require authorisation . A test purchaser is not considered to be a CHIS when the interaction is strictly transactional with no intention to establish or maintain a relationship with the vendor. If the test purchaser is tasked to make multiple visits, build a rapport, and develop a relationship (e.g., to be trusted by a shopkeeper to buy age-restricted goods from the back room), they are acting as a CHIS.

4. The safety and welfare of the CHIS is paramount. Risk assessments should be carried out to determine the risk of tasking a CHIS and the activities being undertaken by the particular person appointed. The risk assessments should be regularly reviewed during the course of the investigation.

CHIS' and Social Media

5. The revised Code of Practice for Covert Human Intelligence Sources at paras 4.29 to 4.35 sets out the position on the use of social media in a potential CHIS context:

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

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

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

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

4.32 Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as "like" or "follow" to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these terms may lead to further interaction with other users and a CHIS authorisation should be obtained if there is an intention to engage in such interaction to obtain, provide access to or disclose information.

4.33 When engaging in conduct as a CHIS, a member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without considering the need for a CHIS authorisation. Full consideration should be given to the potential risks posed by that activity.

4.34 Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with paragraphs 7.15 to 7.21 of this Code should include consideration of the risks arising from that online activity including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take account of any disparity between the technical skills of the CHIS and those of the handler or Authorising Officer, and the extent to which this may impact on the effectiveness of oversight.

4.35 Where it is intended that more than one person will share the same online persona, each individual should be clearly identifiable within the overarching authorisation for that operation. The authorisation should provide clear information about the conduct required of – and the risk assessments in relation to – each individual involved. (See also paragraphs 3.32 to 3.36).”

SECTION 4 - AUTHORISATION PROCEDURES

Completing the forms

1. Once it is decided what type of surveillance is being undertaken, the appropriate forms must be completed and sent to the Authorising Officer for approval.

2. The forms can be found on the Home Office Website RIPA forms - GOV.UK (www.gov.uk). A guide to completing the forms can be found at **Appendix I** (Since the introduction of the POFA local authorities no longer have the power to make urgent oral authorisations - all authorisations, even if urgent, must be made in writing and the relevant judicial approval must be sought.)

3. **Officers contemplating the use of RIPA should first seek the advice of the Monitoring Officer**

Authorising Officers

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

5. Authorised Officers are responsible for assessing and authorising covert directed surveillance and the use of CHIS'.

6. It is the responsibility of Authorising Officers to ensure that when applying for authorisation the principles of necessity and proportionality (see Section 5, paragraph 8) are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy (see Section 5, paragraphs 5.4 – 5.12).

7. Authorising officers are responsible for ensuring that they have received RIPA training prior to authorising RIPA activity. When applying for or authorising RIPA activity under the Policy, officers must also take into account the corporate training and any other guidance issued from time to time by the Monitoring Officer.

Authorising Directed Surveillance

8. Section 28 of RIPA states:

"1)Subject to the following provisions of this Part, the persons designated for the purposes of this section shall each have power to grant authorisations for the carrying out of directed surveillance.

(2)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.

(3)An authorisation is necessary on grounds falling within this subsection if it is necessary—
(a)in the interests of national security;
(b)for the purpose of preventing or detecting crime or of preventing disorder;
(c)in the interests of the economic well-being of the United Kingdom;
(d)in the interests of public safety;
(e)for the purpose of protecting public health;
(f)for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
(g)for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

(4)The conduct that is authorised by an authorisation for the carrying out of directed surveillance is any conduct that—
a)consists in the carrying out of directed surveillance of any such description as is specified in the authorisation; and

(b)is carried out in the circumstances described in the authorisation and for the purposes of the investigation or operation specified or described in the authorisation.

9. To help in deciding whether Directed Surveillance should be authorised please refer to **Flowchart 4**

10. Authorising Officers are referred to **Appendix II** which offers Guidance on things to consider when deciding whether to authorise Directed Surveillance.

Authorising the use of a CHIS

11. Section 29 of RIPA states:

"(1)Subject to the following provisions of this Part, the persons designated for the purposes of this section shall each have power to grant authorisations for the conduct or the use of a covert human intelligence source.

(2)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—
(i)the requirements of subsection (4A), in the case of a source of a relevant collaborative unit;
(ii). . . . . .
(iii)the requirements of subsection (5), in the case of any other source;
and that satisfy such other requirements as may be imposed by order made by the Secretary of State.

(2A)For the meaning of "relevant collaborative unit" in subsection (2)(c)(i), see section 29A.

(3)An authorisation is necessary on grounds falling within this subsection if it is necessary—
(a)in the interests of national security;
(b)for the purpose of preventing or detecting crime or of preventing disorder;
(c)in the interests of the economic well-being of the United Kingdom;
(d)in the interests of public safety;
(e)for the purpose of protecting public health;
(f)for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department; or
(g)for any purpose (not falling within paragraphs (a) to (f)) which is specified for the purposes of this subsection by an order made by the Secretary of State.

(4)The conduct that is authorised by an authorisation for the conduct or the use of a covert human intelligence source is any conduct that—

(a)is comprised in any such activities involving conduct of a covert human intelligence source, or the use of a covert human intelligence source, as are specified or described in the authorisation;

(b)consists in conduct by or in relation to the person who is so specified or described as the person to whose actions as a covert human intelligence source the authorisation relates; and

(c)is carried out for the purposes of, or in connection with, the investigation or operation so specified or described.

(4A)For the purposes of this Part there are arrangements for the source's case that satisfy the requirements of this subsection if such arrangements are in force as are necessary for ensuring—

(a)that there will at all times be a qualifying person who will have day-to-day responsibility for dealing with the source, and for the source's security and welfare (see section 29A for the meaning of "qualifying person") ;

(b)that there will at all times be another qualifying person who will have general oversight of the use made of the source;

(c)that there will at all times be a qualifying person who will have responsibility for maintaining a record of the use made of the source;

(d)that the records relating to the source that are maintained by virtue of paragraph (c) will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State; and

(e)that records maintained by virtue of paragraph (c) that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

(4B). . . . . .

(5)For the purposes of this Part there are arrangements for the source's case that satisfy the requirements of this subsection if such arrangements are in force as are necessary for ensuring—

(a)that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have day-to-day responsibility for dealing with the source on behalf of that authority, and for the source's security and welfare;

(b)that there will at all times be another person holding an office, rank or position with the relevant investigating authority who will have general oversight of the use made of the source;

(c)that there will at all times be a person holding an office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of the source;

(d)that the records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State; and

(e)that records maintained by the relevant investigating authority that disclose the identity of the source will not be available to persons except to

the extent that there is a need for access to them to be made available to those persons.

(6)The Secretary of State shall not make an order under subsection (3)(g) unless a draft of the order has been laid before Parliament and approved by a resolution of each House.

(6ZA)An authorisation for the conduct or the use of a covert human intelligence source does not authorise any criminal conduct in the course of, or otherwise in connection with, the conduct of a covert human intelligence source (but see section 29B for provision for the authorisation of such conduct).

(6A)An authorisation under this section may not have the effect of authorising a covert human intelligence source who is a person designated under section 38 of the Police Reform Act 2002 to establish contact in person with another person.

(7)The Secretary of State may by order—

(a)prohibit the authorisation under this section of any such conduct or uses of covert human intelligence sources as may be described in the order; and

(b)impose requirements, in addition to those provided for by subsection (2), that must be satisfied before an authorisation is granted under this section for any such conduct or uses of covert human intelligence sources as may be so described.

(7A). . . . . .
(7B). . . . . .

(8)In this section "relevant investigating authority", in relation to an authorisation for the conduct or the use of an individual as a covert human intelligence source, means (subject to subsection (9)) the public authority for whose benefit the activities of that individual as such a source are to take place.

(9)In the case of any authorisation for the conduct or the use of a covert human intelligence source whose activities are to be for the benefit of more than one public authority, the references in subsection (5) to the relevant investigating authority are references to one of them (whether or not the same one in the case of each reference).

11. To help in deciding whether use of a CHIS should be authorised please refer to **Flowchart 5**

12. Authorising Officers are referred to **Appendix III** which offers Guidance on things to consider when deciding whether to authorise use of a CHIS.

Next stage after Authorisation

1. Once the Directed Surveillance and / or use of a CHIS has been authorised by an Authorised Officer the stage is to seek approval from the Magistrates Court

SECTION 5 - MAGISTRATES APPROVAL

General

1. The POFA came into force in November 2012. The POFA changed the procedure for the authorisation of local authority surveillance under RIPA.

2. Local authorities are required to obtain the approval of a JP for the use of Directed Surveillance and CHIS.

3. Guidance can be found on the Home Office website providing advice on how local authorities can ensure they are following the correct processes and changes in the legislation Changes to local authority use of RIPA - GOV.UK (www.gov.uk)

Process

4. Once (internally) authorisation has been given / signed by an Authorised Officer, Legal Services will need to make contact with the court listing office and arrange a hearing date and time.

5. The officer who has sought the authorisation will need to attend court, accompanied by Legal Services. The officer will be sworn in, and expected to give evidence under oath.

6. The court will be provided (by Legal Services) with a copy of all the relevant forms and authorisations relevant to the application.

7. The hearing will be in private, and heard by a single JP who will consider the forms and authorisation etc. Since the introduction of the POFA it is no longer sufficient for the local authority to rely on oral evidence – the authorisation and forms must be sufficient by themselves to make the case for approval. The JP can though ask questions of the officer for clarification or for additional reassurances.

8. The JP will decide whether they are satisfied that, at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. They will consider whether there continue to be reasonable grounds. The JP must also be satisfied that the Authorising Officer was of an appropriate level within the Council's structure and that the authorisation was made in accordance with any applicable legal restrictions.

9. JP's may decide to:

• Approve the grant/renewal of the authorisation (the Council can then proceed to use the surveillance technique mentioned therein)

• Refuse to approve the grant/renewal of the authorisation on a technicality (the RIPA authorisation won't take effect and the local authority cannot use the surveillance technique. Technical errors can be rectified without the need to recommence the authorisation process again, then the authority can reapply to the court)

• Refuse to grant/renew and quash the authorisation (the RIPA authorisation won't take effect and the local authority cannot use that surveillance technique. The JP cannot exercise their power to quash an authorisation unless the local authority has been given 2 working days in which to prepare and make further representations).

10. The JP will then complete the Order section of the judicial application/order form. One copy will need to be retained by the Council – this signed documents is the approval.

11. A local authority can only appeal a JPs decision to refuse approval of an authorisation on a point of law by seeking a Judicial Review in the High Court.

Time Limits

12. If the JP approves the authorisation, the authorisation will last:

• For 3 months if the authorisation is for Directed Surveillance, and

• For 12 months if the authorisation is for a CHIS

PART 2 – COMMUNICATIONS DATA

SECTION 6 - ACQUISITION AND DISCLOSURE OF COMMUNICATIONS DATA

1. With effect from 5 February 2019, and in accordance with Part 3 and chapter 2 of Part 6 of the IPA Local Authorities can obtain communications data ('Data') provided that the acquisition of such Data is necessary for the applicable crime purpose; and proportionate to what is sought to be achieved by acquiring it

2. The applicable crime purpose will depend upon whether the communications data being sought is classified as entity data or events data. Where the Data sought is wholly or partly events data the purpose must be for a serious crime. In any other case the Data must be for the purpose of preventing or detecting crime or of preventing disorder.

   Serious crime" means crime where-
   • the offence, or one of the offences, which is or would be constituted by the conduct concerned is an offence for which a person who has reached the age

of 18 and has no previous convictions could reasonably be expected to be sentenced to imprisonment for a term of 1 year or more, or

• the conduct involves the use of violence, results in substantial financial gain or is conduct by a large number of persons in pursuit of a common purpose

3. The Communications data Code of Practice can be accessed here: https://www.gov.uk/government/publications/code-of-practice-for-the-acquisition-and-disclosure-of-communications-data

Important: The Council is NOT Permitted to Intercept any Communications

4. The purpose and effect of the procedure is the same as RIPA i.e. to ensure proper consideration is given to permitting such investigations and to provide protection against a human rights challenge.

5. Applications for Data are subject to independent examination, scrutiny and approval by the IPCO. All applications for Data must be undertaken online through NAFN acting as single point of contact SPOC pursuant to the IPA.

What is 'Communications Data'?

1. The term Communications Data ('Data') includes the "who", "where", and "how" of a communication but not the content i.e. what was said or written. Data is generated, held or obtained in the provision, delivery and maintenance of communications services i.e. postal services or telecommunications services.

2. The Council may only acquire less intrusive types of Data. These are:

•Entity Data – this data describes or identifies the entity. Entities can be individuals and objects (such as mobile phones).

•Events Data –for Data this is limited to communications events which identifies any person, apparatus or location to or from which a communication is transmitted e.g. incoming call records, the location of a mobile phone, or numbers called

3. Data relating to Events data is more intrusive than data relating to Entities Data

SECTION 7 – AUTHORISATIONS

4. The Monitoring Officer shall be appointed as the Council's SRO. The SRO is responsible for

• the integrity of the process in place within the public authority to acquire communications data;

• engagement with authorising officers in the Office for Communications Data Authorisations (where relevant);

• compliance with Part 3 of IPA and with the code, including responsibility for novel or contentious cases;

• oversight of the reporting of errors to the IPCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

• ensuring the overall quality of applications submitted to IPCO by the public authority;

• engagement with the IPCO's inspectors when they conduct their inspections; and

• where necessary, oversight of the implementation of post-inspection action plans approved by the IPCO.

Application Forms

5. The Council will maintain a collaboration agreement with the National Anti-Fraud Network (NAFN). All applications must be made online at https://www.nafn.gov.uk/ NAFN will act as SPOC between both the communications service providers (CSPs) and the Council concerning the request and provision of Data. This is to ensure a centralised and managed approach in making applications to obtain Data and facilitates lawful acquisition of Data and effective co-operation between the Council and CSPs.

6. In addition to being considered by a NAFN SPOC, the applicant for Data must ensure that the Council's SRO is aware of the application being made before it is submitted to an authorising officer in IPCO. The Council's SRO's will be notified to NAFN.

Duration

7. Authorisations to obtain Data are only valid for one month beginning with the date on which the IPCO approval is granted

Renewal and Cancellation

8. An authorisation may be renewed at any time during the month it is valid using the same procedure as used in the original application (including seeking IPCO approval). A renewal takes effect on the date which the authorisation it is renewing expires.

9. The code requires that all authorisations must be cancelled by the Council or IPCO as soon as it is no longer necessary, or the conduct is no longer proportionate to what is sought to be achieved.

10. The Council must notify the SPOC which must cease the authorised conduct.

Retention of Records

11. Applications, authorisations and notices must be retained until the Council has been audited by the Commissioner. Applications must also be retained to allow the Tribunal (see paragraph 14 and 15 below) to carry out its functions.

12. A record must be kept of:

    • the dates of which the authorisation or notice is started or cancelled;

    • any errors that have occurred in the granting of authorisations or giving of notices.

13. A report and explanation of any errors must also be sent to the Commissioner as soon as is practicable. Communications data, and all copies, extracts and summaries of it, must be handled and stored securely and the requirements of the GDPR must be observed. The Monitoring Officer will maintain a centrally retrievable register.

Oversight and Complaints

14. The IPA provides for an IPCO whose remit is to provide independent oversight of the use of the powers contained within the IPA and the code requires any person who uses the powers conferred by the IPA to comply with any request made by the Commissioner to provide any information he requires to enable him to discharge his functions.

15. The IPCO must inform any affected person of any rights that the person may have to apply to the Investigatory Powers Tribunal.