



ASHFIELD DISTRICT COUNCIL

**REGULATION OF INVESTIGATORY
POWERS ACT 2000 (RIPA)**

POLICY AND GUIDANCE

CONTENTS

1. Policy
2. Guidance
3. Appendix A – List of Authorising Officers
4. Appendix B – Flowchart
5. Appendix C – Links to Home Office - Forms
6. Appendix D – Links to Home Office - Codes of Practice
7. Appendix E – Links to Home Office – Guidance for Application at the Magistrates’ Court.

Approved: Cabinet,

2019

Cabinet Minute Reference:

ASHFIELD DISTRICT COUNCIL
POLICY ON REGULATION OF INVESTIGATORY
POWERS ACT 2000 (RIPA)

Ashfield District Council only carries out covert surveillance where such action is justified and endeavours to keep such surveillance to a minimum. It recognises its obligation to comply with RIPA when such an investigation is for one of the purposes set out in that Act and has produced this Guidance document to assist officers undertaking this type of work (“Authorising” and “Investigating Officers”).

Applications for authority

A Chief Officer authorised by the Council (an “Authorising officer”) will consider all applications for authorisation in accordance with RIPA – See **Appendix A** for a list of Authorising Officers.

Any incomplete or inadequate application forms will be returned to the applicant for amendment.

The Authorising Officer shall in particular ensure that:-

- There is a satisfactory reason for carrying out the surveillance
- The serious crime threshold is met
- The covert nature of the investigation is necessary
- Proper consideration has been given to collateral intrusion
- The proposed length and extent of the surveillance is proportionate to the information being sought
- Authorisation from the Head of Paid Service (Chief Executive) is sought where confidential legal/journalistic/medical/spiritual welfare issues are involved
- The authorisations are reviewed and cancelled
- Records of all authorisations are sent to the Service Manager – Legal Services for entry on the Central Register

Once authorisation has been obtained from the Authorising Officer, the Authorising Officer or his/her nominee (e.g. investigating officer) will attend the Magistrates’ Court in order to obtain judicial approval for the authorisation. See flowchart at **Appendix B**.

Training

Each Authorising Officer shall be responsible for ensuring that relevant members of staff within their Directorate are aware of the Act's requirements.

The Shared Legal Service will provide advice and regular updates as well as specific training upon request.

Central register and records

The Service Manager - Legal Services shall retain the Central Register of all authorisations issued by Ashfield District Council.

The Director of Legal and Governance (Monitoring Officer), in conjunction with the Service Manager - Legal Services, will monitor the content of the application forms and authorisations to ensure that they comply with the Act.

Senior Responsible Officer ("SRO")

The SRO is a role required by the Investigatory Powers Commissioner's Office ("IPCO") with oversight of the Council's use of RIPA powers. The SRO is the Director of Legal and Governance (Monitoring Officer) and will only act as an Authorising Officer for the Council in exceptional circumstances to avoid any conflicts with the SRO role.

RIPA Coordinating Officer

The RIPA Co-ordinating Officer has the responsibility for the day-to-day RIPA management and administrative processes observed in obtaining an authorisation and advice thereon and this role is performed by the Service Manager - Legal Services.

REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA) - GUIDANCE

DIRECTED SURVEILLANCE & COVERT HUMAN INTELLIGENCE SOURCE

1. Purpose

The purpose of this guidance is to explain

- the scope of RIPA – Part II;
- the circumstances where it applies; and
- the authorisation procedures to be followed

2. Introduction

2.1 This Act, which came into force in 2000, is intended to regulate the use of investigatory powers exercised by various bodies including local authorities, and ensure that they are used in accordance with human rights. This is achieved by requiring certain investigations to be authorised by an appropriate officer and approved by the judiciary before they are carried out.

2.2 The investigatory powers, which are relevant to a local authority, are directed covert surveillance in respect of specific operations involving criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or are related to the underage sale of alcohol and tobacco and the use of covert human intelligence sources (CHIS). The Act makes it clear for which purposes they may be used, to what extent, and who may authorise their use. There are also Codes of Practice in relation to the use of these powers and the Home Office web site link for these is at **Appendix C and D**.

2.3 Consideration must be given, prior to authorisation as to whether or not the acquisition of private information is necessary and proportionate, i.e. whether a potential breach of a human right is justified in the interests of the community as a whole, or whether the information could be obtained in other ways.

3. Scrutiny and Tribunal

3.1 External

3.1.1 The Council must obtain an order from a Justice of the Peace approving the grant or renewal of any authorisation for the use of directed surveillance or CHIS before the authorisation can take effect and the activity is carried out. The Council can only appeal a decision of the Justice of the Peace on a point of law by judicial review.

3.1.2 The Investigatory Powers Commissioners Office was set up to monitor compliance with RIPA. The IPCO has “a duty to keep under review the exercise and performance by the relevant persons of the powers and duties under Part II of RIPA”, and the Investigatory Powers Commissioner will from time to time inspect the Council’s records and procedures for this purpose.

3.1.3 In order to ensure that investigating authorities are using the powers properly, the Act also establishes a Tribunal to hear complaints from persons aggrieved by conduct, e.g. directed surveillance. Applications will be heard on a judicial review basis. Such claims must be brought no later than one year after the taking place of the conduct to which it relates, unless it is just and equitable to extend this period.

3.1.4 The Tribunal can order:

1. Quashing or cancellation of any warrant or authorisation;
2. Destruction of any records or information obtained by using a warrant or authorisation;
3. Destruction of records or information held by a public authority in relation to any person.

3.1.5 The Council has a duty to disclose to the tribunal all documents they require if any Council officer has:

- Engaged in any conduct as a result of such authorisation;
- Any authorisation under RIPA.

3.2 **Internal Scrutiny**

3.2.1 The Council will ensure that the Senior Responsible Officer is responsible for:

- The integrity of the process in place within the public authority to authorise directed surveillance;
- Compliance with part II of the 2000 Act, Part III of the 1997 Act and with the accompanying Codes of Practice;
- Engagement with the Commissioners and Inspectors when they conduct their inspections; and
- Where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Commissioner.

3.2.2 The Cabinet will receive updates on the use of the Act at least once a year and set/review the Council’s policy and guidance documents where necessary. They will also consider internal reports on use of the Act where necessary to ensure that it is being used consistently with the Council’s policy and that the policy

remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations.

3.3 Unauthorised Activities

3.3.1 If an Officer is concerned that surveillance/CHIS activity is taking place and there is no authorisation under RIPA, he/she should notify the Director of Legal and Governance (Monitoring Officer) immediately.

3.3.2 If any activity is deemed to be unauthorised, it will be reported to the IPCO.

4. Benefits of RIPA authorisations

4.1 The Act states that if authorisation confers entitlement to engage in a certain conduct and the conduct is in accordance with the authorisation, then it will be lawful for all purposes. Consequently, RIPA provides a statutory framework under which covert surveillance activity can be authorised and conducted compatibly with Article 8 of the Human Rights Act 1998 – a person's right to respect for their private and family life, home and correspondence.

4.2 Material obtained through properly authorised covert surveillance is admissible evidence in criminal proceedings.

5. Definitions

5.1 'Covert' is defined as surveillance carried out in such a manner that is calculated to ensure that the person subject to it is unaware that it is or may be taking place. (s.26 (9)(a)).

5.2 'Covert human intelligence source' (CHIS) is defined as a person who establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining/providing access to/disclosing, information obtained through that relationship or as a consequence of the relationship. (s.26 (8)).

5.3 'Directed surveillance' is defined as covert but not intrusive and undertaken:

- for a specific investigation or operation;
- in such a way that is likely to result in the obtaining of private information about any person;
- other than by way of an immediate response (s.26 (2)).

5.4 'Private information' includes information relating to a person's private or family life but has a wide meaning, not excluding business or professional activities.

5.5 'Intrusive' surveillance is covert surveillance that is carried out in relation to anything taking place on any residential premises or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or using a surveillance device. **Ashfield District Council may not authorise such surveillance.**

5.6 'Authorising Officer' in the case of local authorities these are specified as Assistant Chief Officers (and more senior officers), Assistant Heads of Service, Service Managers or equivalent, responsible for the management of an investigation (see Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 (SI 2010/521)). Ashfield District Council has appointed the Chief Executive and Directors as "Authorising Officers". Please refer to **Appendix A** for a list of Authorising Officers for Ashfield District Council.

6. When does RIPA apply?

6.1 Where the directed covert surveillance of an individual or group of individuals, or the use of a CHIS, **is necessary for the purpose of preventing or detecting crime or of preventing disorder.**

6.2 The Council can only authorise **Directed Surveillance** to prevent and detect conduct which constitutes one or more criminal offences. The criminal offences must be punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment or be an offence under:

- a) S.146 of the Licensing Act 2003 (sale of alcohol to children);
- b) S.147 of the Licensing Act 2003 (allowing the sale of alcohol to children);
- c) S.147A of the Licensing Act 2003 (persistently selling alcohol to children);
- d) S.7 of the Children and Young Persons Act 1933 (sale of tobacco, etc, to persons under eighteen).

6.3 CCTV

The normal use of CCTV is not usually covert because members of the public are informed by signs that such equipment is in operation. However, authorisation should be sought where it is intended to use CCTV covertly and in a pre-planned manner as part of a specific investigation or operation to target a specific individual or group of individuals. Equally a request, say by the police, to track particular individuals via CCTV recordings may require authorisation (from the police).

The Council's CCTV is managed by Newark and Sherwood District Council pursuant to a Service Level Agreement.

6.4 Online Covert Activity

Reviewing open source sites does not require authorisation unless the review is carried out with some regularity, usually when creating a profile, in which case directed surveillance authorisation will be required. If it becomes necessary to breach the privacy controls and become, for example, a "friend" on a Facebook site, with the investigating officer utilising a false account concealing his/her identity as a Council Officer for the purposes of gleaning intelligence, this is a covert operation intended to obtain private information and should be authorised, at a minimum, as directed surveillance. If the investigator engages in any form of relationship with the account operator then the investigator becomes a CHIS requiring authorisation as such and management by a Controller and Handler with a record being kept and a risk assessment created.

Where the serious crime threshold is not met in relation to an investigation, surveillance of social media sites could amount to a breach of an individual's Article 8 rights for which there is no protection offered by RIPA. Officers using social media sites as part of an investigation should seek advice from the Shared Legal Team as to when an authorisation for directed surveillance or CHIS would be required.

The Revised Code of Practice for Covert Surveillance and Property Interference (August 2018) provides the following guidance in relation to online covert activity:

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.

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

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

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

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

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and

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

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

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

7. Covert Human Intelligence Source

7.1 Put simply, this means the use of members of the public, undercover officers or professional witnesses to obtain information and evidence.

7.2 The RIPA definition (section 26) is anyone who:

- a) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs b) or c);
- b) covertly uses such a relationship to obtain information or provide access to any information to another person; or
- c) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

Any reference to the conduct of a CHIS includes the conduct of a source which falls within a) to c) or is incidental to it.

References to the use of a CHIS are references to inducing, asking or assisting a person to engage in such conduct.

7.3 Section 26(9) of RIPA goes on to define:

- a) a purpose is covert, in relation to the establishment or maintenance of a personal or other relationship, if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of that purpose; and
 - b) a relationship is used covertly, and information obtained as mentioned in s 26(8) (c) above and is disclosed covertly, if, and only if it is used or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.
- 7.4 With any authorised use of a CHIS, the Council must ensure that arrangements are in place for the proper oversight and management of the CHIS, this includes appointing individual officers as Handlers and Controllers in relation to the CHIS (s.29(5)(a) and (b)).
- 7.5 There is a risk that an informant who is providing information to the Council voluntarily may in reality be a CHIS even if not tasked to obtain information covertly. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised in the 2000 Act, not whether or not the CHIS is asked to do so by the Council. When an informant gives repeat information about a suspect or about a family and it becomes apparent that the informant may be obtaining the information in the course of a neighbourhood or family relationship, it may mean that the informant is in fact a CHIS. Legal advice should always be sought in such instances before acting on any information from such an informant.
- 7.6 Detailed advice regarding applications for use of a CHIS are set out at paragraph 8.1.5 below. In the event that the use of CHIS is considered, the Service Manager - Legal Services must be consulted before any steps are taken to engage the CHIS.

The Revised Code of Practice for Covert Human Intelligence Sources (August 2018) provides the following guidance in relation to online covert activity:

4.11 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, whether by publicly open websites such as an online news and social networking service, or more private exchanges such as e-messaging sites, 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. A directed surveillance authorisation should also be considered, unless the acquisition of that information is or will be covered by the terms of an applicable CHIS authorisation.

4.12 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 (such as a CHIS) 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.

4.13 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, though 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.

Example 1: An HMRC officer intends to make a one-off online test purchase of an item on an auction site, to investigate intelligence that the true value of the goods is not being declared for tax purposes. The officer concludes the purchase and does not correspond privately with the seller or leave feedback on the site. No covert relationship is formed and a CHIS authorisation need not be sought.

Example 2: HMRC task a member of the public to purchase goods from a number of websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. The individual is required to engage with the seller as necessary to complete the purchases. The deployment should be covered by a CHIS authorisation because of the intention to establish a relationship for covert purposes.

4.14 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 it is intended for an officer of a public authority or a CHIS to engage in such interaction to obtain, provide access to or disclose information.

Example 1: An officer maintains a false persona, unconnected to law enforcement, on social media sites in order to facilitate future operational research or investigation. As part of the legend building activity he “follows” a variety of people and entities and “likes” occasional posts without engaging further. No relationship is formed and no CHIS authorisation is needed.

Example 2: The officer sends a request to join a closed group known to be administered by a subject of interest, connected to a specific investigation. A directed surveillance authorisation would be needed to cover the proposed covert monitoring of the site. Once accepted into the group it becomes apparent that further interaction is necessary. This should be authorised by means of a CHIS authorisation.

4.15 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 authorisation. Full consideration should be given to the potential risks posed by that activity.

4.16 Where use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with section 6.13 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.

4.17 Where it is intended that more than one officer will share the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved. (See also paragraph 3.23)

7.7 Juvenile Sources

Special safeguards apply to the use or conduct of juvenile sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under the age of 16 years be authorised to give information against his parents or any person who has parental responsibility for him. The duration of a juvenile CHIS is **four** months. The Regulation of Investigatory Powers (Juveniles) Order 2000 SI No. 2793 contains special provisions which must be

adhered to in respect of juvenile sources. Any authorisation of a juvenile CHIS must be made by the Head of Paid Service (Chief Executive) or an Officer authorised on his behalf.

7.8 **Vulnerable Individuals**

A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any individual of this description should only be authorised to act as a source in the most exceptional circumstances. Any authorisation of a juvenile CHIS must be made by the Head of Paid Service (Chief Executive) or an Officer authorised on his behalf.

8. **Authorisations (see flowchart at Appendix B)**

8.1 **Applications for directed surveillance**

8.1.1 All application forms must be completed fully with all the required details to enable the Authorising Officer to make an informed decision.

An authorisation provides for one period of Directed Surveillance lasting three months. If a proposed operation is expected to be completed in a shorter timeframe, the authorisation will still last for three months but an appropriately early review should be carried out and, if the operation is no longer necessary or proportionate the authorisation should be cancelled.

Officers should ensure they are using the most up-to-date forms for RIPA Authorisations. Application forms are available on the Home Office website:

<https://www.gov.uk/government/collections/ripa-forms--2>

No authorisation shall be granted unless the Authorising Officer is satisfied that the investigation is:

- **Necessary** for the purpose of preventing or detecting crime. It must be a criminal offence punishable whether summarily or on indictment by a maximum sentence of at least 6 months imprisonment or related to the underage sale of alcohol or tobacco (see para 6);
- **Proportionate to the ultimate objective**. This has 3 elements, namely:
 - a) that the method of surveillance proposed is not excessive to the seriousness of the matter under investigation;
 - b) the method used must be the least invasive of the target's privacy; and

- c) the privacy of innocent members of the public must be respected and collateral intrusion minimised (see 8.1.2).
- **Collateral Intrusion** is intrusion on, or interference with, the privacy of persons other than the subject of the investigation;
- **No other form of investigation would be appropriate.**

Necessity: Covert surveillance cannot be said to be necessary if the desired information can reasonably be obtained by overt means. It must also be necessary for the purpose of preventing or detecting conduct which constitutes one or more criminal offences as set out in paragraph 6 above.

Proportionality: The method of surveillance proposed must not be excessive in relation to the seriousness of the matter under investigation. It must be the method which is the least invasive of the target's privacy.

Collateral intrusion, which affects the privacy rights of innocent members of the public, must be minimised and use of the product of the surveillance carefully controlled so as to respect those rights.

The grant of authorisation should indicate that consideration has been given to the above points. Advice should be obtained from the Shared Legal Service where necessary.

- 8.1.2 The Authorising Officer must also take into account the risk of '**collateral intrusion**'. The application must include an **assessment** of any risk of collateral intrusion for this purpose.

Steps must be taken to avoid unnecessary collateral intrusion and minimise any necessary intrusion.

Those carrying out the investigation must inform the Authorising Officer of any unexpected interference with the privacy of individuals who are not covered by the authorisation, as soon as these become apparent.

Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to what is sought to be achieved.

The Authorising Officer should also fully understand the capabilities and sensitivity levels of any equipment being used to carry out directed surveillance so as to properly assess the risk of collateral intrusion in surveillance techniques.

8.1.3 **Special consideration in respect of confidential information**

Particular attention is drawn to areas where the subject of surveillance may reasonably expect a high degree of privacy, e.g. where confidential information is involved.

Confidential information consists of matters subject to legal privilege, communication between Members of Parliament and another person on constituency matters, confidential personal information or confidential journalistic material. (ss 98-100 Police Act 1997).

Legal privilege

Generally, this applies to communications between an individual and his/her legal adviser giving of legal advice in connection with, or in contemplation of, legal proceedings. Such information is unlikely ever to be admissible as evidence in criminal proceedings.

If in doubt, the advice of the Director of Legal and Governance (Monitoring Officer) or the Service Manager - Legal Services should be sought in respect of any issues in this area.

Confidential personal information

This is oral or written information held in (express or implied) confidence, relating to the physical or mental health or spiritual counselling concerning an individual (alive or dead) who can be identified from it. Specific examples provided in the codes of practice are consultations between a health professional and a patient, discussions between a minister of religion and an individual relating to the latter's **spiritual welfare** or matters of **medical or journalistic confidentiality**.

Confidential journalistic material

This is material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence.

It should be noted that matters considered to be confidential under RIPA may not necessarily be properly regarded as confidential under section 41 Freedom of Information Act 2000.

In such cases, where it is likely that knowledge of confidential information will be acquired, the use of covert surveillance is subject to a higher level of authorisation and therefore may only be authorised by the Head of Paid Services (Chief Executive) or an officer authorised by him for this purpose. Authorisation can only be granted where there are exceptional and compelling circumstances that make the authorisation necessary.

8.1.4 **Notifications to Inspector/Commissioner**

The following situations must be brought to the Inspector/Commissioner's attention at the next inspection:

- Where an officer has had to authorise surveillance in respect of an investigation in which he/she is directly involved;
- Where legally privileged information has been acquired
- Where a lawyer is the subject of an investigation or operation;
- Where confidential personal information or confidential journalistic information has been acquired and retained.

8.1.5 **Applications for CHIS**

Applications for CHIS are made in the same way as for directed surveillance except that the serious crime threshold of investigating criminal offences with a sentence of at least 6 months in imprisonment does not apply. The authorisation must specify the activities of the CHIS and that the authorised conduct is carried out for the purposes of, or in connection with, the investigation or operation so specified.

The Authorising Officer must be satisfied that the use of a CHIS has been risk assessed and is proportionate to what is sought to be achieved by that use and it must be necessary for the prevention and/or detection of crime.

A record must be kept of the matters mentioned in s29(5) and the Source Records Regulations (SI 2000/2725). The Justice of the Peace must be satisfied that the provisions of section 29(5) have been complied with.

Section 29(5) requires:

- “ (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.”*

All application forms must be fully completed with the required details with a risk assessment to enable the authorising officer to make an informed decision.

8.1.6 **Judicial Approval of Authorisations**

Once the Authorising Officer has authorised the Directed Surveillance or CHIS, the Authorising Officer (or his/her nominee) who completed the application form should contact the Magistrates' Court to arrange a hearing for the authorisation to be approved by a Justice of the Peace.

The Authorising Officer (or his/her nominee) will provide the Justice of the Peace with a copy of the original authorisation and the supporting documents setting out the case. This forms the basis of the application to the Justice of the Peace and should contain all information that is relied upon.

In addition the Authorising Officer (or his/her nominee) will provide the Justice of the Peace with a partially completed judicial application/order form.

The hearing will be in private and the Authorising Officer (or his/her nominee) will be sworn in and present evidence as required by the Justice of the Peace. Any such evidence should be limited to the information in the authorisation.

The Justice of the Peace will consider whether he/she is satisfied that at the time the authorisation was given there were reasonable grounds for believing that the authorisation or notice was necessary and proportionate and whether that continues to be the case. They will also consider whether the authorisation was given by the appropriate designated person at the correct level within the Council and whether (in the case of directed surveillance) the crime threshold has been met.

The Justice of the Peace can:

- a) **Approve the grant of the authorization**, which means the authorisation will then take effect;

- b) **Refuse to approve the grant of the authorisation**, which means the authorisation will not take effect but the Council could look at the reasons for refusal, make any amendments and reapply for judicial approval.
- c) **Refuse to approve the grant of the authorisation and quash the original authorisation**. The court cannot exercise its power to quash the authorisation unless the applicant has at least 2 business days from the date of the refusal in which to make representations.

Guidance for applications to the Magistrates' Court can be found via the link at **Appendix E**.

8.1.7 **Working in partnership with the Police**

Authorisation can be granted in situations where the police rather than the Council require the surveillance to take action, as long as the behaviour complained of, meets all criteria to grant and in addition is also of concern to the Council. Authorisation cannot be granted for surveillance requested by the police for a purely police issue.

The Police may authorise RIPA without Magistrates' Court approval; if an urgent situation arises and RIPA authorisation would be required urgently the Council should contact the Police.

9. **Duration and Cancellation**

- An authorisation for **directed surveillance** shall cease to have effect (if not renewed) **3 months** from the date the Justice of the Peace approves the grant
- If renewed the authorisation shall cease to have effect 3 months from the expiry date of the original authorisation.
- An authorisation for **CHIS** shall cease to have effect (unless renewed) **12 months** from the date the Justice of the Peace approves the grant or renewal.

This does not mean that the authorisation should necessarily be permitted to last for the whole period so that it lapses at the end of this time. The Authorising Officer, in accordance with s.45 of the Act, must cancel each authorisation as soon as that officer decides that the surveillance should be discontinued.

Authorisations continue to exist even if they have ceased to have effect. Authorisations, therefore, must be cancelled if the directed surveillance as a whole no longer meets the criteria upon which it was authorised.

The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained and kept with the cancellation form.

The cancellation form should detail what surveillance took place, if there was any collateral intrusion, what evidence was obtained and how it is to be managed, any risks to a CHIS. Details relating to the retention of records is set out in paragraph 13 below.

10. Reviews

The Authorising Officer should review all authorisations at intervals determined by him/herself. This should be as often as necessary and practicable. The reviews should be recorded.

If the directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at review to include the identity of these individuals. A review would be appropriate specifically for this purpose.

Particular attention should be paid to the possibility of obtaining confidential information.

11. Renewals

Any Authorised Officer may renew an existing authorisation on the same terms as the original at any time before the original ceases to have effect.

The renewal must then be approved by the Justice of the Peace, before the expiry of the original authorisation, in the same way the original authorisation was approved.

The process outlined in paragraph 8.1.6 should be followed for renewals.

A CHIS authorisation must be thoroughly reviewed at regular intervals before it is renewed.

12. Central Register of Authorisations

12.1 All authorities must maintain the following documents:

- Copy of the application and a copy of the authorisation and Order made by the Magistrates' Court together with any supplementary documentation and notification of the approval given by the Authorising Officer;
- A record of the period over which the surveillance has taken place;
- The frequency of reviews prescribed by the Authorising Officer;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation and Order made by the Magistrates' Court and supporting documentation submitted when the renewal was requested;
- The date and time when any instruction to cease surveillance was given;
- The date and time when any other instruction was given by the Authorising Officer.

12.2 To comply with 12.1, the Service Manager - Legal Services holds the central register of all authorisations issued by officers of Ashfield District Council. The original copy of every authorisation, renewal and cancellation issued should be lodged immediately with the Service Manager - Legal Services in an envelope marked 'Private and Confidential'. Any original authorisations and renewals taken to the Magistrates' Court should be retained by the Council, the Court must only keep copies of the authorisations or renewals.

12.3 The Council must also maintain a centrally retrievable record of the following information:

- type of authorisation
- date the authorisation was given
- date the approval Order was given by the Magistrates' Court
- name and rank/grade of the Authorising Officer
- unique reference number of the investigation/operation
- title (including brief description and names of the subjects) of the investigation/operation

- details of renewal
- dates of any approval Order for renewal given by the Justice of the Peace
- whether the investigation/operation is likely to result in obtaining confidential information
- date of cancellation
- whether the authorisation was granted by an individual directly involved in the investigation
- Magistrates' Court Information
- Where any application is refused, the grounds for refusal as given by the issuing authority or Judicial Commissioner:
- a record of whether, following a refusal of any application by a Judicial Commissioner, there is an appeal to the Investigatory Powers Commissioner;
- where there is such an appeal and the Investigatory Powers Commissioner also refuses the issuing of an application, the grounds for refusal given.

These records will be retained for at least 3 years and will be available for inspection by the Investigatory Powers Commissioner's Office..

13. **Retention of records**

The Council must ensure that arrangements are in place for the secure handling, storage and destruction of material obtained through the use of directed surveillance or CHIS.

Authorising Officers, through their relevant Data Controller, must ensure compliance with the appropriate data protection requirements under the Data Protection Act 2018 and any relevant codes of practice relating to the handling and storage of material.

14. **Complaints procedure**

- 14.1 The Council will maintain the standards set out in this guidance and the Codes of Practice (**See Appendix C and D**). The Chief Investigatory Powers Commissioner has responsibility for monitoring and reviewing the way the Council exercises the powers and duties conferred by RIPA.
- 14.2 Contravention of the Data Protection Act 2018 may be reported to the Information Commissioner. Before making such a reference, a complaint concerning a breach of this guidance should be made using the Council's own internal complaints procedure. To request a complaints form, please contact the Council at Council Offices, Urban Road, Kirkby-in-Ashfield, Nottinghamshire, NG17 8DA, or telephone 01623 450000, or e-mail to customerservices@ashfield.gov.uk
- 14.3 The 2000 Act establishes an independent Tribunal. The Tribunal has full powers to investigate and decide any case within its jurisdiction. Details of the relevant complaints procedure can be obtained from the following address:

Investigatory Powers Tribunal

PO Box 33220

London

SW1H 9ZQ

0207 035 3711

Email: info@ipt-uk.com

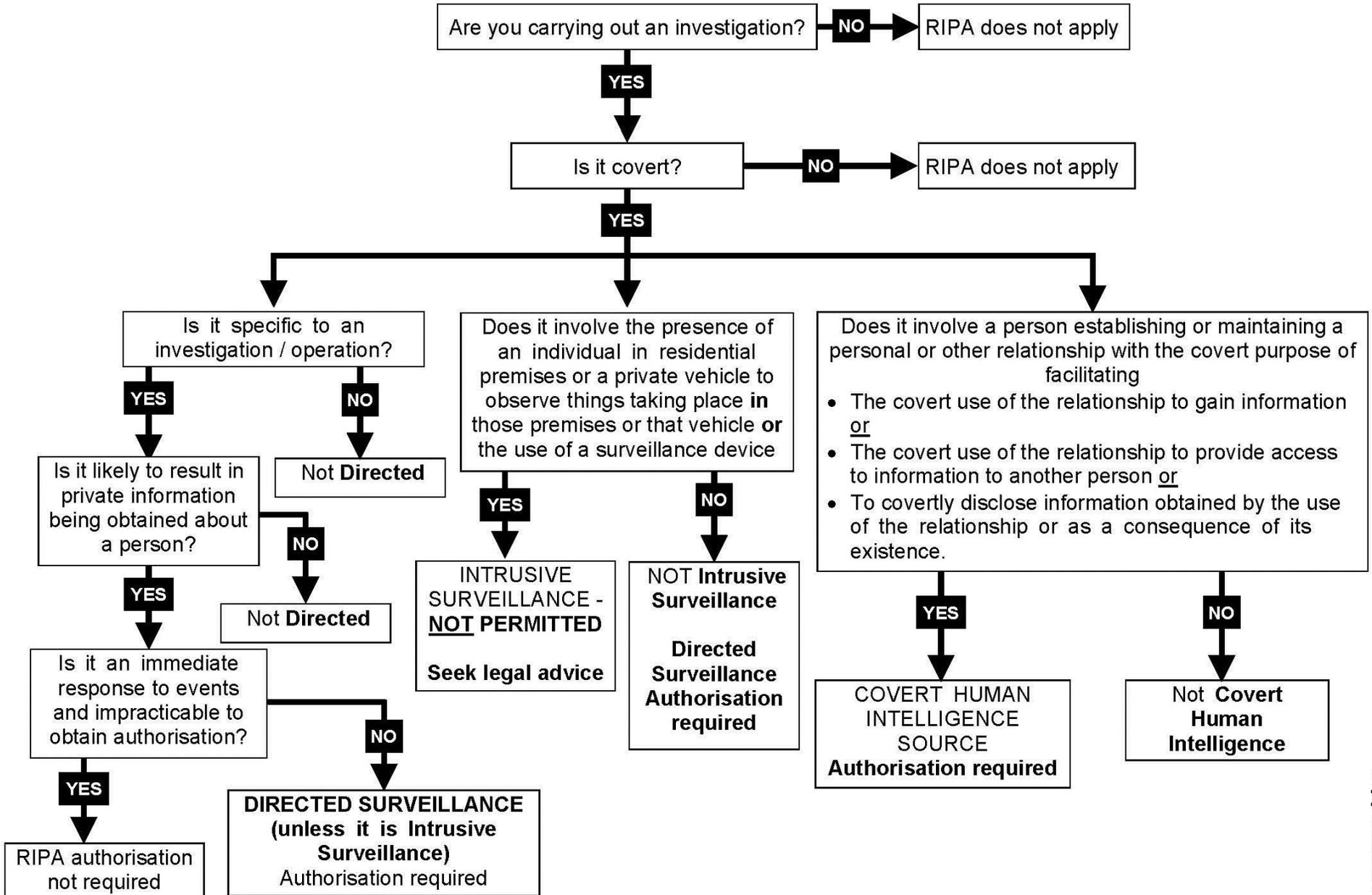
Appendix A – Authorising Officers

Job Title	Contact No.
Chief Executive, or interim Chief Executive (Head of Paid Service)	01623 450000 Ext: 4250
Director of Revenues and Business Transformation or interim Director	01623 450000 Ext: 4203
Director of Housing and Assets, or interim Director	01623 450000 Ext: 2891
Interim Director of Place and Communities, or interim Director	01623 450000 Ext: 4374

For authorisations relating to Juveniles (para 7.7), Vulnerable CHIS (para 7.8) or Journalistic/Confidential Material (Para 8.1.3):	
Chief Executive (Head of Paid Service), or interim Chief Executive	01623 450000 Ext: 4250
In exceptional circumstances:	
Director of Legal and Governance (Monitoring Officer) & RIPA Senior Responsible Officer	01623 450000 Ext: 4009

DIRECTED SURVEILLANCE

Regulation of Investigatory Powers Act 2000 - Do you need Authorisation?



APPENDIX C

Forms

See Home Office website:

<https://www.gov.uk/government/collections/ripa-forms--2>

APPENDIX D

Codes of Practice

See Home Office website:

<https://www.gov.uk/government/collections/ripa-codes>

APPENDIX E

Guidance for Applications at the Magistrates' Court

See Home Office website:

<https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa>