The Regulation of Investigatory Powers Act 2000 - Policy and Procedure

Delegation & Review:	RIPA reviewed by Audit & Governance Committee (with effect from March 2025)
Policy created	
Policy updated	September 2024, February 2026
Policy created by	Monitoring Officer
Policy review due	February 2027

St Albans City and District Council

The Regulation of Investigatory Powers Act 2000: Policy and Procedure on the use of covert surveillance and "covert human intelligence sources"

Statement of Intent: St Albans City and District Council attaches a high value to the privacy of citizens. It will adhere to the letter and to the spirit of the Act and will comply with this Code.

POLICY

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 ("RIPA") is designed to ensure that public bodies respect the privacy of members of the public when carrying out investigations, and that privacy is only interfered with where the law permits and there is a clear public interest justification.

2. What does RIPA do?

2.1 RIPA places controls on the use of certain methods of investigation. In particular, it regulates the use of surveillance and "covert human intelligence sources". This guide covers these aspects of the Act. Further guidance will be issued on other aspects of the Act if necessary.

The policy and procedure on the use of covert surveillance and "covert human intelligence sources" is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA'), The Protection of Freedoms Act 2012 and Codes of Practice issued by the Home Office pursuant to Section 71 of RIPA. The authoritative position on RIPA is, of course, the Act itself, regulations and the Home Office's Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources.

2.2 RIPA's main implications for the Council are in respect of covert surveillance by Council officers and the use of "covert human intelligence sources". (A covert human intelligence source is someone who uses a relationship with a third party in a secretive manner to obtain or give information – for instance an informer or someone working "under cover".)

2.3 An authorisation for directed surveillance can only be obtained for the purpose of a specific investigation or operation in so far as that investigation is necessary

on the grounds specified in the 2000 Act. RIPA can only be used for specific "core functions" which are the "specific public functions" undertaken by the Council such as Environmental Protection or Food Safety. RIPA cannot be used for "ordinary functions" which are undertaken by all authorities such as employment issues, contractual arrangements, etc. These "ordinary functions" are covered by Data Protection Act 2018 and the Information Commissioner's Employment Practices Code. The disciplining of an employee is not a "core function" although related criminal proceedings might be. The protection for the Council to ensure evidence is not excluded which is afforded under the 2000 Act may be available in relation to associated criminal investigations, so long as the activity is deemed to be necessary and appropriate.

2.4 Local Authorities investigating criminal offences have powers to gain access to communications data – that is, information held by telecommunications or postal service providers about the use of their services by persons who are the subject of criminal investigations. When using these powers officers must always have regard to the Home Office Guidance – Acquisition and Disclosure of Communication Data Code

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

2.5 This document and the related forms can be found on the Council's RIPA SharePoint site, accessible by authorised officers.

2.6 The Council is a member of the National Anti-Fraud Network (NAFN) and they will obtain such communications data on the provision of appropriate authorisation.

2.7 The Council has had regard to the Codes of Practice produced by the Home Office in preparing this Policy & Procedure. If any doubt arises, the Home Office Code of Practice should be consulted. CHIS and Covert Surveillance Codes of Practice:

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

2.8 There is also further guidance in respect of the judicial approval process and the crime threshold issued by the Home Office:- https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

2.9 If the correct RIPA procedures are not followed, evidence may be disallowed by the courts; the matter must be reported by the Monitoring Officer to the Investigatory Powers Commissioner; a complaint of maladministration could be made to the Local Government and Social Care Ombudsman, and/or the Council could be ordered to pay compensation. Such action would, of course, harm the reputation of the Council and will, undoubtedly, be the subject of adverse press and media interest. It is essential, therefore, that all Council staff involved with

RIPA, comply with this Policy & Procedure and any further guidance that may be issued, from time to time, by the Monitoring Officer.

3. Some definitions

3.1 "*Surveillance*"

Close observation, especially of suspected criminal

3.2 *"Covert"*

Concealed, done secretly

3.3 "*Covert surveillance*"

Surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place;

3.4 *"Directed surveillance"*

Directed surveillance is defined in RIPA as surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance (i.e. where the circumstances make it impractical to seek authorisation. An example might be where an officer on patrol or carrying out other duties sees a person acting suspiciously and decides to watch them surreptitiously to see whether they are intending to commit a crime.)

Private information in relation to a person includes any information relating to his private or family life.

3.5 *"Intrusive surveillance"*

Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

a. is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

b. involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

4. RIPA and Surveillance – what is not covered

4.1 General observation forms part of the duties of some Council officers. They may, for instance, be on duty at events in the City and District and will monitor the crowd to maintain public safety and prevent disorder. Environmental Health Officers might covertly observe and then visit a shop as part of their enforcement function. Such observation may involve the use of equipment merely to reinforce normal sensory perception, such as binoculars, or the use of cameras, where this does not involve systematic surveillance of an individual. It forms a part of the everyday functions of law enforcement or other public bodies. This low-level activity will not usually be regulated under the provisions of RIPA.

4.2 Neither do the provisions of the Act cover the use of overt CCTV surveillance systems. Members of the public are aware that such systems are in use, for their own protection, and to prevent crime. There is a separate Code of Practice adopted by the Council to govern use of CCTV.

4.3 The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear does not constitute directed surveillance. In any of these circumstances, the perpetrator would normally be regarded as having forfeited any claim to privacy. In these circumstances, an authorisation is unlikely to be required.

5. RIPA and Surveillance – What is covered?

5.1 The Act is designed to regulate the use of “covert” surveillance. Covert surveillance means surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place. Strictly speaking, only two types of covert surveillance are regulated by RIPA – “directed” and “intrusive” surveillance. However, where the purpose of a surveillance operation is to obtain private information about a person, the authorisation procedures set out in this guide should be followed and the surveillance treated as being “directed”.

5.2 Directly employed Council staff and external agencies working for the Council are covered by RIPA for the time they are working for the Council. All external agencies must, therefore, comply with RIPA, and the work carried out by agencies on the Council’s behalf must be properly authorised by one of the Council’s designated Authorising Officers.

5.3 <u>What RIPA Does and Does Not Do</u>

RIPA does:

- Require prior authorisation, from the Council's authorising officers and Magistrate's Court, of directed surveillance.
- Prohibit the Council from carrying out intrusive surveillance.
- Require authorisation of the conduct and use of a CHIS.
- Require safeguards for the conduct and use of a CHIS.

RIPA does not:

- Prejudice or disapply any existing powers 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 via the DVLA or to get information from the Land Registry as to the ownership of a property.

6. What is "directed surveillance"?

6.1 Directed surveillance is defined in RIPA as surveillance which is covert, but not intrusive, and undertaken:

a) for the purposes of a specific investigation or operation;

b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and

c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Part to be sought for the carrying out of the surveillance.

Private information in relation to a person includes any information relating to his private or family life.

6.2 Directed surveillance is conducted where it involves the observation of a person or persons with the intention of gathering private information to produce a detailed picture of a person's life, activities and associations. However, it does not include covert surveillance carried out by way of an immediate response to events or circumstances which, by their very nature, could not have been foreseen. For example, a plain clothes police officer would not require an authorisation to conceal himself and observe a suspicious person who he comes across in the course of a patrol.

6.3 Directed surveillance does not include any type of covert surveillance in residential premises or in private vehicles. Such activity is defined as "intrusive surveillance" and is dealt with in section 7.

6.4 In practice, the sort of directed surveillance which the Council might undertake would include covert surveillance connected with the prosecution of serious offences including public health offences or in connection with investigating cases of substantial fraud. You should treat anything involving the use of concealed cameras or anything involving keeping covert observation on premises or people as potentially amounting to directed surveillance. If you are unsure, please take advice from the Solicitor to the Council, who is also the Monitoring Officer.

6.5 Directed surveillance **must** be properly authorised in accordance with the procedure set out in section 9.

6.6 You should treat any covert surveillance which is likely to intrude upon anyone's privacy to more than a marginal extent as directed surveillance, even if it does not fall within the strict terms of the definition – for instance where surveillance is not part of a specific investigation or operation. If the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded may engage privacy considerations, RIPA considerations may need to be considered.

6.7 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 necessary.

6.8 Care should be taken on covert surveillance of social networking sites. Digital investigation may be relatively easy to conduct but this does not remove the need for authorisation. Care must be taken to understand how the social networking site is being used. Service providers may have different approaches to privacy settings.

6.9 Whilst it is responsibility of the individual to set privacy settings to protect unsolicited access to private information, and even though data may be deemed published and no longer under the control of the author, it is unwise to regard it as "open source" or publicly available; the author has a reasonable expectation of privacy if access controls are applied. In some cases data may be deemed to be private communication still in transmission (instant messages for example). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. However repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

6.10 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 openly available within the public domain. However, in some circumstances privacy implications still apply. This is because the intention when making such information available is 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.

6.11 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 wider audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

6.12 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, such as a 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. However, 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 whether or not the information was shared online.

6.13 In order to determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a directed 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:

a. Whether the investigation is directed towards an individual or an organisation

b. Whether it is likely to result in obtaining private information about a person or a group of people. (This may include personal data such as names, telephone numbers and address details.)

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

d. Whether the information obtained will be recorded and retained.

e. Whether the information is likely to provide an observer with a pattern of lifestyle.

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

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

h. 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.

6.14 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.

6.15 Officers also refer to the Council's Use of Social Media in Investigations Policy.

7. What is intrusive surveillance?

7.1	**An important warning: the Council cannot authorise intrusive surveillance.**

7.2 Intrusive surveillance is defined as covert surveillance that:

a. is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

b. involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

7.2 In essence, intrusive surveillance amounts to intrusion into people's homes or vehicles either physically or by means of a surveillance device.

7.3 Intrusive surveillance cannot be undertaken without authorisation and the Council cannot authorise intrusive surveillance. Bodies such as the Police and Customs and Excise can authorise intrusive surveillance. If you are asked by another agency to co-operate with intrusive surveillance, you should seek advice from the Monitoring Officer immediately. Where other authorities say that they are authorised to undertake intrusive surveillance but need our co-operation, we need to check that their authorisation is in order.

8. What is a covert human intelligence source?

8.1 A covert human intelligence source is someone who establishes or maintains a relationship with a person for the purpose of covertly obtaining or disclosing information. In practice, this is likely to cover the use of an informer or Council officer to strike up a relationship with someone as part of an investigation to obtain information "under cover".

8.2 Someone who volunteers information to the Council, either as a complainant (for instance, about anti-social behaviour or a breach of planning regulations) or out of civic duty, is unlikely to be a covert human intelligence source. If someone is keeping a record, say, of neighbour nuisance, this will not amount by itself to use of a covert human intelligence source. However, if we are relying on, say, a

neighbour to ask questions with a view to gathering evidence, then this may amount to use of a covert human intelligence source.

8.3 The use by the Council of covert human intelligence sources is expected to be extremely rare and, for that reason, this guide does not deal with the issues to which they give rise. If you are contemplating use of a covert human intelligence source, please take advice from the Monitoring Officer before putting your plan into action.

8.4 An authorisation would be required to establish a relationship on a social networking site as it is inadvisable to do so for a covert purpose without authorisation. Where you proposed to engage with others online without disclosing your identity a CHIS authorisation may be needed**.** Using photographs of other persons without their permission to support a false identity infringes other laws.

9. Authorising Directed Surveillance: The Rules

9.1 It is crucial that all directed surveillance is properly authorised. Failure to secure proper authorisation and to comply with this procedure could lead to evidence being excluded by the courts and to complaints against the Council. The Council is subject to audit and inspection by the Investigatory Powers Commissioner and it is important that we can demonstrate compliance with RIPA and with this code. Again, please note that the Council cannot authorise intrusive surveillance – see section 7.

9.2 **Who can authorise directed surveillance?** Regulations made under the Act say that the most junior level at which authorisations can only be given is by what it refers to as “Director, Service Manager or equivalent”. For the purposes of this Code, authorisations may only be given by the officers identified in the Appendix to this Guide referred to as “authorising officers”.

The authorisation of directed surveillance likely to obtain confidential information or the deployment of a juvenile or vulnerable person (by virtue of mental or other condition) as a CHIS requires authorisation by the most senior local authority officer. This is the Chief Executive or in her absence the Deputy Chief Executive.

If there is any doubt regarding sufficiency of rank please contact the the Monitoring Officer, or in their absence their Deputies, who will be able to advise you.

9.3 **On what grounds can directed surveillance be authorised?** Directed surveillance can only be authorised by local authorities for the purpose of preventing or detecting criminal offences that are punishable, whether on summary conviction or indictmentby a maximum term of at least 6 months imprisonment or are related to the underage sale of alcohol and tobacco or nicotine inhaling products.

Local authorities are no longer able to provide verbal authority for the use of RIPA techniques. All authority must be in writing.

9.4 **When do you need Magistrates' Approval?**

A list of potential offences is attached which is by no means definitive and will be subject to constant review (see Appendix 7).

(The Police have wider powers to authorise directed surveillance).

Please note that surveillance has to be in accordance with the law, necessary and proportionate for the crime and disorder purpose. If you can just as well carry out an investigation by means which do not involve directed surveillance, then you should use them.

(See chapter 4 para 4.42 to 4.47 of the Home Office Covert Surveillance and Property Interference Revised Code of Practice, August 2018)

9.4 **Is the proposed surveillance proportionate?** Authorisation should not be sought, and authority should not be given unless you are satisfied that the surveillance is proportionate. You should make sure that any interference with privacy is justified by the end being sought. If the benefit to be obtained from surveillance is marginal, or if the problem you are seeking to tackle is not very serious, you should think very carefully about whether the use of surveillance is proportionate. We should not "use a sledgehammer to crack a nut."

9.5 **Is the proposed surveillance discriminatory?** The Council is under a legal obligation to avoid either direct or indirect discrimination in carrying out its functions. As surveillance can interfere with rights contained in the European Convention on Human Rights, discrimination can also amount to a breach of the Human Rights Act. You should be sensitive to this issue and ensure that you apply similar standards to seeking or authorising surveillance regardless of ethnic origin, sex or sexual orientation, disability, age etc. You should be alert to any assumptions about people from different backgrounds which may not even be consciously held.

9.6 **Might the surveillance involve "collateral intrusion"?** In other words, might the surveillance intrude upon the privacy of people other than those who are the subject of the investigation. You should be sensitive of the privacy rights of third parties and consider very carefully whether the intrusion into their privacy is justified by the benefits of undertaking the surveillance.

9.7 **Might the Surveillance involve private information?**

9.7.1 The 2000 Act states that private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others,

such as family and professional or business relationships. Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public. Non-private data will also include the attributes of inanimate objects such as the class to which a cargo ship belongs.

9.7.2 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by the Council of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly where accessing information on social media websites.

Example: *Two people holding a conversation on the street or in a bus may have a reasonable expectation of privacy over the contents of that conversation, even though they are associating in public. The contents of such a conversation should therefore still be considered as private information. A directed surveillance authorisation would therefore be appropriate for the Council to record or listen to the conversation as part of a specific investigation or operation.*

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

Example: *Council officers wish to drive past a café for the purposes of obtaining a photograph of the exterior. Reconnaissance of this nature is not likely to require a directed surveillance authorisation as no private information about any person is likely to be obtained or recorded. However, if the Council wished to repeat the exercise, for example to establish a pattern of occupancy of the premises by any person, the accumulation of information is likely to result in the obtaining of private information about that person and a directed surveillance authorisation would be required.*

9.7.4 Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him/her and others that s/he comes into contact, or associates, with.

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

Similarly, although overt town centre CCTV cameras do not normally require authorisation, if a particular camera is being used for a specific purpose, which involves prolonged surveillance on a particular person, authorisation will be required. The way a person runs his/her business may also reveal information about his or her private life and the private lives of others.

9.8 **Might the surveillance involve acquiring access to any confidential or religious material?** If so, then the surveillance will require a particularly strong justification and arrangements need to be put in place to ensure that the information obtained is kept secure and only used for proper purposes. Confidential material might include legal or financial records, or medical records. Where there is a possibility that access to confidential or religious material might be obtained, the authorisation of the Chief Executive should be sought.

9.9 **What is confidential information?**

9.9.1 Special consideration must be given to authorisations that involve confidential personal information. Where such material has been acquired and retained, the matter should be reported to the Monitoring Officer so that they can inform the Investigatory Powers Commissioner's Office (IPCO) or Inspector during their next inspection and the material made available to them if requested.

9.9.2 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling of a person (whether living or dead) who can be identified from it. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation.

Examples include consultations between a health professional and a patient, or information from a patient's medical records.9.10Any authorisations when knowledge of confidential information is likely to be acquired must be authorised by the Chief Executive or in their absence their deputy.

9.11 **Online covert activity**

9.11.1 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for Local 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 Local 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 council officers in identifying when such authorisations may be appropriate.

9.11.2 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.

9.11.3 Where a person acting on behalf of the Council 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).*

9.11.4 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 the Council 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.

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 the Council 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.

9.11.5 Whether the Council 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 the Council 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 section 7 above)*.

Example 1: *A council 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 council 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: *The Council 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.*

9.11.6 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 in section 7 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.

9.11.7 Internet searches carried out by a third party on behalf of the Council, or with the use of a search tool, may still require a directed surveillance authorisation.

Example: *Researchers within a local 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 local 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.*

9.12 Intrusive Surveillance

This is when it:

- is covert;
- relates to anything taking place on residential premises or in any private vehicle;
- and, involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

Residential premises includes any part of premises which are being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation. It includes hotel accommodation. However, common areas to which a person has access in connection with their use or occupation of accommodation are excluded from the definition of residential premises.

Examples of common areas of residential premises which are excluded would include:

- a communal stairway in a block of flats;
- a hotel reception area or dining room;
- the front garden or driveway of premises readily visible to the public.

A private vehicle is any vehicle which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This includes, for example, a company car, owned by a leasing company and used for business and pleasure by the employee of a company.

Local authorities are not allowed to carry out intrusive surveillance and

Therefore, no Council officer can authorise a covert surveillance operation if it involves intrusive surveillance as defined above.

9.14 Where authorisation is not required

Some surveillance activity does not constitute directed surveillance under RIPA and no directed surveillance authorisation can be obtained for such activity. Such activity includes:

- covert surveillance by way of an immediate response to events;
- covert surveillance as part of general observation activities;
- covert surveillance not relating to the statutory grounds specified by RIPA;
- overt use of CCTV;
- the overt or covert recording of an interview with a member of the public where it is made clear that the interview is entirely voluntary and that the interviewer is a Council officer.
- the covert recording of suspected noise nuisance where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear. In the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy.

PROCEDURE

10. Authorising Directed Surveillance: The Procedure

10.1 Applying for authorisation.

10.1.1 Applications for authorisation must be made on the correct form. The form to seek authorisation is reproduced at Appendix 2 to this Guide. It, and other forms and information, may also be found on the Home Office web site at www.homeoffice.gov.uk (see Appendix 6).

10.1.2 A written application for authorisation for directed surveillance should describe in detail any conduct to be authorised and the purpose of the investigation or operation. The application should also include:

- the reasons why the authorisation is necessary in the particular case and on the grounds (e.g. for the purpose of preventing or detecting crime) listed in Section 28(3) of the 2000 Act;
- the reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the nature of the surveillance;
- the identities, where known, of those to be the subject of the surveillance;
- an explanation of the information which it is desired to obtain as a result of the surveillance;
- the details of any potential collateral intrusion and why the intrusion is justified;
- the details of any confidential information that is likely to be obtained as a consequence of the surveillance.
- the level of authority required (or recommended where that is different) for the surveillance; and
- a subsequent record of whether authority was given or refused, by whom and the time and date.

  A risk assessment should also be carried out and an observations log should be completed. A risk assessment pro forma is attached as Appendix 8.

10.1.3 Authorising Officers should clearly state what kind of activity is required and authorised.

10.1.4 Following the authorisation an application must then be made to a Magistrates Court for a Hearing. Please contact the Legal Department who will arrange this. See the flowchart at Appendix 6.

10.1.5 An authorisation of directed surveillance or a CHIS does not take effect until it has been approved and signed by a Magistrate. The dates and times of signatures by both the Authorising officer should be recorded. Care should be taken to accurately record the expiry date of the authorisation.

10.2 **Duration of authorisations**

10.2.1 A written authorisation granted by a Magistrate will cease to have effect (unless renewed) at the end of a period of **three months** beginning with the day on which it took effect.

10.2.2 Even though authorisations cease to have effect after three months, you should not simply leave them to run out. When the surveillance ceases to be necessary, you should always follow the cancellation procedure. See section 10.5. Where surveillance has ceased, we must be able to match each authorisation with a cancellation.

10.3 **Reviews**

10.3.1 Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The maximum period between authorisation and review, and between reviews, should be four weeks. The more significant the infringement of privacy, the more frequent should be the reviews. The results of a review should be recorded on the central record of authorisations (see paragraph 11). Particular attention is drawn to the need to review authorisations frequently where the surveillance provides access to confidential information or involves collateral intrusion.

10.3.2 In each case authorising officers within the Council should determine how often a review should take place. This should be as frequently as is considered necessary and practicable.

10.3.3 The form to record a review of an authorisation is reproduced at Appendix 3 to this Guide.

10.4 **Renewals**

10.4.1 If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue for the purpose for which it was given, s/he may apply again to a Magistrate renew it in writing for a further period of **three months**. Authorisations may be reviewed more than once if still considered necessary and proportionate and approved by a Magistrate.

10.4.2 A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an

end. However you should take account of factors which may delay the renewal process such as intervening weekends or the availability of the relevant authorising officer and a Magistrate to consider the application.

10.4.3 All applications for the renewal of an authorisation for directed surveillance should be made on the form attached as Appendix 4 to this guide and should record:

- whether this is the first renewal or every occasion on which the authorisation has been renewed previously;
- any significant changes to the information given in the original application for authorisation;
- the reasons why it is necessary to continue with the directed surveillance;
- the content and value to the investigation or operation of the information so far obtained by the surveillance;
- the results of regular reviews of the investigation or operation.

10.4.4 Authorisations may be renewed more than once, if necessary, and the renewal should be kept/recorded as part of the central record of authorisations (see section 11).

10.5 Cancellations

10.5.1 The authorising officer who considered the authorisation which the Magistrate approved or renewed must cancel the authorisation it if he is satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of authorising officer. If in doubt about who may cancel an authorisation, please consult the Monitoring Officer.

10.5.2 Cancellations are to be affected by completion of the form in Appendix 5 to this Guide.

10.5.2 N.B. Please note the warning in paragraph 10.2.2 that there must be a completed cancellation for each authorisation once surveillance has been completed. An authorisation cannot simply be allowed to expire.

10.6 Ceasing of surveillance activity

10.6.1 As soon as the decision is taken that directed surveillance should be discontinued, the instruction must be given to those involved to stop all surveillance of the subject(s). The date and time when such an instruction was given should be included in the Notification of Cancellation form.

11. Record Keeping and Central Record of Authorisations

11.1 In all cases in which authorisation of directed surveillance is given, the Service Head is responsible for ensuring that the following documentation is kept safely for a period of at least three years from the date of authorisation:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the Magistrate;
- 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 by a Magistrate, together with the supporting documentation submitted when the renewal was requested;
- the date and time when any instruction was given by the authorising officer.

11.2 In addition, copies the following must be sent to the Monitoring Officer immediately upon completion:

- all completed forms authorising directed surveillance;
- all completed forms authorising renewal of directed surveillance;
- all completed forms cancelling directed surveillance.

The Monitoring Officer will allocate the forms with a unique reference number. The forms will be kept by the Monitoring Officer who will review them at least every twelve months.

12. Authorising Use of Covert Human Intelligence Sources

12.1 Similar principles and procedures apply to authorising the use of covert human intelligence sources. If it becomes apparent that their use is more than very exceptional, detailed guidance will be published and circulated. For the present, officers' attention is drawn to the explanation of the nature of a covert human intelligence source in Section 8. If you think you might be using, or might use, a covert human intelligence source, please contact the Monitoring Officer, who will advise on the principles to be applied, the authorisation procedure, record keeping etc. For the avoidance of doubt, the Council will comply, so far as applicable, with the model guidance issued by the Home Office.

13. Access to Communications data

13.1 There are stringent controls placed on access by the Council to "communications data". The Council is not entitled to obtain access to the content of communications between third parties but can, in some circumstances, obtain information relating to the use of a communications service. "Communications services" include telecom providers, postal services and internet service providers.

13.2 This is a complex area, procedurally and legally. Access to communications data can only be obtained through the Council's designated "single point of contact" ("SPOC") for communications data. At the present time we do not actually exercise these powers as we do not have a designated "SPOC".

14. Further Information

14.1 There is much helpful information on the Home Office web site about RIPA. See www.homeoffice.gov.uk (see Appendix 6).

14.2 The Monitoring Officer is happy to advise further on issues connected with RIPA. Departments need to consider what their training needs are in this area. Regular training courses are arranged to keep officers up to date.

Judith Adamson, Solicitor
Monitoring Officer
February 2026

Appendices

Appendix 1: Authorising Officers under Regulation of Investigatory Powers Act 2000.

Appendix 2: Form for Authorising directed covert surveillance.
https://www.gov.uk/government/publications/application-for-use-of-directed-surveillance

Appendix 3: Form for Review of authorisation for directed covert surveillance.
https://www.gov.uk/government/publications/review-of-use-of-directed-surveillance

Appendix 4: Form for Renewal of authorisation for directed covert surveillance.
https://www.gov.uk/government/publications/renewal-form-for-directed-surveillance

Appendix 5: Form for Cancellation of authorisation for directed covert surveillance.
https://www.gov.uk/government/publications/cancellation-of-use-of-directed-surveillance-form

Appendix 6: Links to various information on Home Office Website http://www.homeoffice.gov.uk/ and Flow Chart showing links to the Acts, Codes of Practice and the Forms.

Home

▼

Advance Search

▼

RIPA Forms or RIPA Codes of Practice

Appendix 7: list of Acts which may be relevant for Section 28 of the Regulation of Investigatory Powers Act 2000.

Appendix 8: RIPA Risk Assessment Pro-Forma.
\\sadc-vm-fs01\global\RIPA\RIPA risk assessment pro-forma.pdf

Appendix 1: Authorisation of Officers under Regulation of Investigatory Powers Act 2000

I hereby approve the following as designated officers under the Regulation of Investigatory Powers Act 2000 to give authorisations for directed covert surveillance and the use of a covert human intelligence source:

I hereby approve the following as authorising officers under the Regulation of Investigatory Powers Act 2000 to give authorisations for directed covert surveillance and the use of a covert human intelligence source:

Monitoring Officer
Head of Legal Shared Services
Solicitor – Regulatory Team Leader
Solicitor – Property & Estates Team Leader
Employed Barrister – Procurement Team Leader

Amanda Foley
Chief Executive

St Albans City and District Council
4th April 2024

Appendix 7: list of Acts which may be relevant for Section 28 of the Regulation of Investigatory Powers Act 2000

(Offences which are punishable whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment)

Licensing Act 2003 sections 136 and 137 unauthorised licensable activity etc.

Planning (Listed Buildings and Conservation) Areas Act 1990 sections 7 and 9

Town and Country Planning Act 1990 sections 194, 196D and 330(5)

Health and Safety at Work Act 1974 section 33 (1) (a), (b), (c), (e), (f), (g), (j), (k), (l), (m), (o)

Food Safety Act 1990 sections 8 and 35 (2)

Fraud Act 2006

Protection from Eviction Act 1977 section 1

Gambling Act 2005 sections 33, 37 and 342

Environmental Protection Act 1990 section 33(1)