Herefordshire Council

Approved: June 2021 Version: 2
Last revised: October 2024
Review date: October 2027
Category
Owner: Legal services
Target audience: council officers

Regulation of Investigatory Powers Act 2000 (RIPA) Policy and Procedures (including non-RIPA surveillance)

Regulation of Investigatory Powers Act 2000 (RIPA) - Policy and Procedures (including non-RIPA surveillance)

GENERAL STATEMENT OF POLICY

This policy document explains how Herefordshire Council will comply with the Regulation of Investigatory Powers Act 2000 ('RIPA') and Investigatory Powers Act (IPA) in relation to directed surveillance, use of covert human intelligence sources and the acquisition of communications data. In addition, situations where surveillance is performed outside of RIPA. This Policy is supplementary to the:

Regulation of Investigatory Powers Act (RIPA) 2000 -
http://www.legislation.gov.uk/ukpga/2000/23/contents

Investigatory Powers Act 2016 (IPA)
Investigatory Powers Act 2016 (legislation.gov.uk)

Human Rights Act -
Human Rights Act 1998 (legislation.gov.uk)

Guidance on the use of covert surveillance or human intelligence sources by public authorities under part 2 of the Regulation of Investigatory Powers Act (RIPA) 2000.-
https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligencesources-codes-of-practice

Guidance to local authorities on the judicial approval process for RIPA and the crime threshold for directed surveillance -
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/118173/local-authority-england-wales.pdf

1.0 BACKGROUND

1.1 The primary function of central and local government regulation and enforcement is to protect the individual, the environment, and a variety of groups such as consumers and workers. At the same time, carrying out regulatory functions in an equitable, practical and consistent manner helps to promote a thriving national and local economy, and to prevent and detect crime and disorder.

1.2 The Regulation of Investigatory Powers Act 2000 (RIPA) came into effect in September 2000. RIPA sets out a regulatory framework for the use of covert surveillance techniques by public authorities. If such activities are conducted by council officers, then RIPA regulates them in a manner which is compatible with the European Convention on Human Rights (ECHR), particularly Article 8 (the right to respect for private and family life). IPA came into force in 2006 and regulates what form of communications data can be obtained by local authorities.

1.3 Sections 37 and 38 of the Protection of Freedoms Act 2012 (the Act) came into force on 1 November 2012. Under the Act, local authority authorisations and notices for the use of particular covert techniques (direct surveillance, covert human intelligence sources (CHIS)

and the acquisition of communications data) can only be given effect once an order approving the authorisation or notice has been granted by a Justice of the Peace (JP).

1.4 In addition amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 ("the 2010 Order") mean that a local authority can now only grant an authorisation under RIPA for the use of directed surveillance where the local authority is investigating particular types of criminal offences. These are criminal offences which attract a maximum custodial sentence of 6 months or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933 (sale of tobacco and alcohol to underage children).

1.5 Herefordshire Council will on occasion need to use covert surveillance in order to carry out its enforcement functions effectively. Examples of enforcement activities which may require the use of RIPA includes trading standards, community and fire safety, fraud investigations and child protection.

1.6 The council takes seriously its responsibilities as a regulatory authority and will at all times act in accordance with the law, ensuring that any regulatory and enforcement action it takes is lawful, necessary and proportionate.

1.7 The council will also undertake surveillance activities where the qualifications for RIPA is not met applied (as per paragraph 3.2) and this Policy applies to such surveillance.

2.0 SCOPE AND DEFINITIONS

2.1 This policy applies to all Herefordshire Council services.

2.2 The main purpose of RIPA is to ensure that the relevant investigatory powers are used in accordance with human rights. These powers are:

- interception of communications
- acquisition of communications data (e.g. billing data)
- intrusive surveillance (on residential premises/in private vehicles)
- directed surveillance in the course of specific operations
- use of covert human intelligence sources (informants etc)
- access to encrypted data

2.3 By working in conjunction with other, pre-existing legislation, the Act ensures the following points are clearly covered:

- purposes to which relevant powers may be used
- which authorities can use the powers
- authorisation of the use of the powers
- the use that can be made of material gained
- independent judicial oversight
- a means of redress for the individual where powers are breached

2.4 RIPA limits local authorities to using 3 covert techniques for the purposes of the prevention or detection of crime or prevention of disorder. These techniques are:

- **Directed surveillance** - surveillance which is covert but not intrusive, and which is undertaken for the purposes of a specific investigation or a specific operation, in such a manner as is likely to result in obtaining information about a person – whether or not the target of the investigation/operation.

- A **covert human intelligence source (CHIS) -** undercover officers, public informants and people who make test purchases.

- **Communications data (CD)** - is the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content of what was said or written). RIPA groups CD into 3 parts:

  - 'traffic data' (which includes information about where the communications are made or received);
  - 'service use information' (such as the type of communication, time sent and its duration); and
  - 'subscriber information' (which includes billing information such as the name, address and bank details of the subscriber of telephone or internet services).

2.5 The council must be satisfied that there is an identifiable offence before authorising any covert surveillance. In addition the key tests in any application for authorisation are:

- Necessity
- Proportionality and
- Risk of collateral intrusion

3.0 DIRECTED SURVEILLANCE

3.1 Directed surveillance is defined in Section 26(2) of RIPA as surveillance which is covert, but not intrusive, and undertaken:

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

- in such a manner as it is likely to result in the obtaining of **private information** (Section 13) about the person (whether or not one specifically identified for the purposes of the investigation or operation); and

- otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practical for an authorisation under Part II of RIPA to be sought for the carrying out of the surveillance

3.2 The Council will only use directed surveillance to investigate a crime and where the criminal offence being investigated meets one of the following conditions:

- The offence is punishable, whether on summary conviction or on indictment to a maximum term of at least 6 months of imprisonment, or
- Section 146, 147 or 147A of the Licensing Act 2003 or
- Section 7 of the Children's and Young Persons Act 1933

3.3 The crime threshold applies only to the authorisation of **directed surveillance** by local authorities under RIPA, not to the authorisation of local authority use of CHIS or their acquisition of CD.

3.4 No officer of the council will undertake intrusive surveillance. Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle and which involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

3.5 Surveillance operations will only be carried out by officers who have received appropriate training in human rights and the Act.

3.6 No officer within the council will undertake directed surveillance without prior or emergency authorisation (see section 7).

3.7 The use of directed surveillance under RIPA will not be authorised to investigate matters that do not involve criminal offences or to investigate low-level offences that do not meet the threshold test.

3.8 The use of non-RIPA directed surveillance shall be authorised in accordance with this guidance. This relates to surveillance for non-core functions (non public functions) of the Council (for example, functions related to contracts, as a land owner or related to employees). In all aspects the Council will comply other legislation requirements (Article 6 of the Human Rights Act 1998 and Data Protection Act 2018) and the guidance issued 31 January 2019 to Investigatory Powers Commissioner which includes 'a non-statutory authorisation process that runs in parallel to RIPA approvals'. In practice, this means the Council will follow the same process for non-RIPA directed surveillance other than seeking judicial approval.

4.0 COVERT HUMAN INTELLIGENCE SOURCE (CHIS)

4.1 A CHIS is defined by section 26(8) of RIPA as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating the doing of anything falling within the following points;

- covertly uses such a relationship to obtain information or to provide access to any information to another person: or
- covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship and
- authorisations will only be given to officers who have undergone appropriate training in human rights and the Act.

4.2 The authorisation for the conduct and use of a CHIS may include:

- someone employed or engaged by the council to hide their true identity or motivation and covertly use a relationship to obtain information and disclose it to the local authority (an undercover officer); or

- a member of the public who provides a tip-off to a local authority and is asked to go back and obtain further information by establishing or continuing a relationship whilst hiding their true motivation (an informant).

4.3 Vulnerable individuals (a person who is 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 or protect himself against significant harm or exploitation) may be authorised to act as a CHIS **only in the most exceptional circumstances.** Authorisation must be given by the chief executive or in his/her absence the director adults and communities and he/she will only do so after taking advice from the solicitor to the council.

4.4 Authorisation will only be given for the use of a covert human intelligence source, when the activity is necessary:

- to prevent or detect crime,
- in the interests of public safety,
- for the economic well-being of the UK,
- the purposes of national security
- for protecting public health.

Or is revenue related or specified by the Secretary of State.

4.5 Public volunteers

In many cases involving human sources, a relationship will not have been established or maintained for a covert purpose. Many sources merely volunteer or provide information that they have observed or acquired other than through a relationship, without being induced, asked, or tasked by a public authority. This means that the source is not a CHIS for the purposes of the 2000 Act and no authorisation under the 2000 Act is required.

Example 1: A member of the public volunteers a piece of information to a member of a public authority regarding something they have witnessed in their neighbourhood. The member of the public would not be regarded as a CHIS. They are not passing information as a result of a relationship which has been established or maintained for a covert purpose.

Example 2: A caller to a confidential hotline (such as Crimestoppers, the HMRC Fraud Hotline, the Anti-Terrorist Hotline, or the Security Service public telephone number) reveals that they know of criminal or terrorist activity. Even if the caller is involved in the activities on which they are reporting, the caller would not be considered a CHIS as the information is not being disclosed on the basis of a relationship which was established or maintained for that covert purpose. However, should the caller be asked to maintain their relationship with those involved and to continue to supply information (or it is otherwise envisaged that they will do so), an authorisation for the use or conduct of a CHIS may be appropriate.

4.6 Professional or statutory duty

Certain individuals will be required to provide information to public authorities or designated bodies out of professional or statutory duty. For example, employees within organisations regulated by the money laundering provisions of the Proceeds of Crime Act 2002 are required to report suspicious transactions. Similarly, financial officials, accountants or company administrators may have a duty to provide information that they have obtained by virtue of their position to the Serious Fraud Office.

4.7 Any such regulatory or professional disclosures should not result in these individuals meeting the definition of a CHIS, as the business or professional relationships from which the information derives will not have been established or maintained for the covert purpose of disclosing such information.

4.8 Furthermore, this reporting is undertaken 'in accordance with the law' and therefore any interference with an individual's privacy (Article 8 rights) will be in accordance with Article 8(2) ECHR.

4.9 This statutory or professional duty, however, would not extend to the situation where a person is asked to provide information which they acquire as a result of an existing professional or business relationship with the subject but that person is under no obligation to pass it on. For example, a travel agent who is asked by the police to find out when a regular client next intends to fly to a particular destination is not under an obligation to pass this information on. In these circumstances, a CHIS authorisation may be appropriate.

4.10 Tasking not involving relationships

Tasking a person to obtain information covertly may result in authorisation under Part II of the 2000 Act being appropriate. However, this will not be true in all circumstances. For example, where the tasking given to a person does not require that person to establish or maintain a relationship for the purpose of obtaining, providing access to or disclosing the information sought or where the information is already within the personal knowledge of the individual, that person will not be a CHIS.

Example: A member of the public is asked by a member of a public authority to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is therefore not available. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual. Identifying when a human source becomes a CHIS

4.11 Individuals or members of organisations (e.g. travel agents, housing associations and taxi companies) who, because of their work or role have access to personal information, may voluntarily provide information to public authorities on a repeated basis and need to be managed appropriately. Public authorities must keep such human sources under constant review to ensure that they are managed with an appropriate level of sensitivity and confidentiality, and to establish whether, at any given stage, they should be authorised as a CHIS.

4.12 Determining the status of an individual or organisation is a matter of judgement by the public authority. Public authorities should avoid inducing individuals to engage in the conduct of a CHIS either expressly or implicitly without obtaining a CHIS authorisation.

Example: Mr Y volunteers information to a member of a public authority about a work colleague out of civic duty. Mr Y is not a CHIS at this stage as he has not established or maintained (or been asked to establish or maintain) a relationship with his colleague for the covert purpose of obtaining and disclosing information. However, Mr Y is subsequently contacted by the public authority and is asked if he would ascertain certain specific information about his colleague. At this point, it is likely that Mr Y's relationship with his colleague is being maintained and used for the covert purpose of providing that information.

A CHIS authorisation would therefore be appropriate to authorise interference with the Article 8 right to respect for private or family life of Mr Y's work colleague.

4.13 However, the tasking of a person should not be used as the sole benchmark in seeking a CHIS authorisation. It is the activity of the CHIS in exploiting a relationship for a covert purpose which is ultimately authorised by the 2000 Act, whether or not that CHIS is asked to do so by a public authority. It is possible, therefore, that a person will become engaged in the conduct of a CHIS without a public authority inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where a public authority is aware that a third party is independently maintaining a relationship (i.e. "self-tasking") in order to obtain evidence of criminal activity, and the public authority intends to make use of that material for its own investigative purposes.

4.14 The use of a CHIS by the council is unlikely. These activities will only be undertaken where there is no other reasonable and less intrusive means of obtaining the information.

5.0 COMMUNICATIONS DATA

5.1 The term 'communications data' embraces the 'who', 'when' and 'where' of a communication but not the content, not what was said or written. It is information about a communication - not the communication itself.

5.2 Under RIPA a local authority can only authorise the acquisition of the less intrusive types of communications data such as service use and subscriber information. Under **no circumstances** can local authorities be authorised to obtain traffic data under RIPA.

5.3 In the case of communications data the RIPA authorisation or notice will be scrutinised by a single point of contact (a 'SPoC'). The SPoC is either an accredited individual or a group of accredited individuals trained to facilitate lawful acquisition of communications data and effective co-operation between a public authority and Communication Service Providers (CSPs). An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requests for CD are made. Herefordshire council uses National Anti-Fraud Network (NAFN) as the SPoC.

5.4 Under RIPA it is against the law for a business to intercept any electronic communication on its, or anyone else's, system. There are some exceptions to this:

- Interception is authorised under a warrant (this does not apply to local authorities)
- where the interception takes place with consent
- where the interception is connected with the operation of the communications service itself

5.5 Interception for business related workplace monitoring may be applicable in certain circumstances by the Telecommunications (Lawful Business Practice) (Interception of Communications) Regulations 2000. The regulations are designed to meet the legitimate needs of businesses to manage their information systems, making use of the capabilities of modern communications technology, but in a way that is consistent with high standards of privacy.

5.6 Interception of Council telecommunications will only be made in accordance with the Regulations, and following procedures agreed by the Director of Legal & Governance. Interception may be carried out in the following circumstances:

- To establish the existence of facts or to ascertain compliance with regulatory or self regulatory practices (e.g. to keep records of communications where the specific facts are important, such as being able to prove that a customer has been given certain advice).

- To check the standards are being achieved or ought to be achieved (e.g. to check the quality of e-mail responses sent by members of staff to customer enquiries or for staff training).

- To prevent or detect crime (e.g. to check that employees or others are not involved in defrauding the Council).

- To investigate or detect unauthorised use of the telecommunications system. Note that interception that is targeted at personal communications that do not relate to the business is not allowed regardless of whether the use of the system for such communications is authorised.

- To ensure the security of the system and its effective operation (e.g. to check for viruses or other threats to the system or to enable automated processes such as caching or load distribution).

5.7 The Council will make all reasonable efforts to inform potential users that interceptions may be made.

6.0 COVERT SURVEILLANCE OF SOCIAL NETWORKING SITES

6.1 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.

6.2 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, 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 Home Office Covert Human Intelligence Sources code of practice provide detail on where a CHIS authorisation may be available for online activity).

6.3 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.

6.4 As set out in paragraph 6.5 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.

6.5 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.

6.6 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.

***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.*

6.7 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
- 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.

6.8 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 3.0).

***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.*

7.0 APPLICATION AND AUTHORISATION (See appendix 1 & 2)

7.1 At the start of an investigation, council officers will need to satisfy themselves that what they are investigating is a criminal offence. Directed surveillance is an invasive technique and at the point it is decided whether or not to authorise its use, it must be clear that the threshold is met and that it is necessary and proportionate to use it.

7.2 The applicant will complete a written RIPA application form found at https://www.gov.uk/government/collections/ripa-forms--2 and the authorisation form (see appendix 1) setting out for consideration by the authorising officer or, for communications data the designated person; why use of a particular technique is necessary and proportionate in their investigation. This authorising officer or designated person will consider the application, recording his/her considerations and countersign the form if he/she believes the statutory tests are met.

7.3 In cases where, through the use of surveillance, it is likely that knowledge of confidential information will be acquired, the use of surveillance is subject to a higher level of authorisation. The chief executive or in his/her absence director economy, communities and corporate will authorise surveillance activity where confidential information is likely to be acquired, he or she will do so only after taking advice from the solicitor to the council.

7.4 "Confidential information" is defined for the purposes of RIPA as matters subject to legal privilege, confidential personal information or confidential journalistic material. Confidential material must not be copied or retained unless for a specific purpose – e.g. use in evidence in proceedings and may only be disseminated following advice from the Head of Legal Services/Solicitor to the Council,

7.5 After the form has been countersigned the local authority must seek judicial approval for their RIPA authorisation or notice. The Justice of the Peace (JP) will decide whether a local authority grant or renewal of an authorisation or notice to use RIPA should be approved and it will not come into effect unless and until it is approved by a JP.

7.6 The time limits for authorised applications are three months for directed surveillance and twelve months for a CHIS (one month if the CHIS is under 18). Authorisations and notices for communications data will be valid for a maximum of one month from the date the JP has approved the grant. This means that the conduct authorised should have been commenced or the notice served within that month.

8.0 Reviews

Authorisations should be reviewed regularly to assess the need for surveillance to continue. The results of a review should be recorded in the central record of authorisations. Particular attention should be paid to reviews where the surveillance provides access to confidential information or involves collateral intrusion.

It is the responsibility of the authorising officer to determine how often a review should take place and this should be as frequently as is considered necessary and practicable

9.0 Renewals

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 of which it was given, he may renew it in writing for a further period of three months. Magistrate approval must then be obtained prior to expiry of the original authorisation in order for activity to continue.

All applications for renewal of an authorisation should record:-

(a) whether this is the first renewal or every occasion on which the authorisation has been renewed previously;

(b) any significant changes to the information contained in the original application;

(c) the reasons why it is necessary to continue the surveillance;

(d) the content and value to the investigation or operation of the information so far obtained from the surveillance;

(e) the result of regular reviews of the investigation or operation.

Renewal records should be kept as part of the central record of authorisations.

10. Cancellations

The authorising officer who granted or last renewed the authorisation must cancel it as soon as it no longer meets the criteria for which it was originally authorised. In any event, it will expire after 3 months (4 months for CHIS).

Where the authorising officer is no longer available the person who is taking over that role will be responsible.

Ceasing surveillance activity.

As soon as the decision to cease directed surveillance is taken all those involved must be directed to stop surveillance of the subject. The date and time when such an instruction was given should be recorded in the central record of authorisations and the notification of cancellation where relevant which should also cancel the remained unused duration of the authorisation.

11. Data Retention

RIPA documents should be kept in the central filing system held by legal with a working copy held by team/ applying officer. Documents should be destroyed after 6 years or after any completed prosecution court case whichever is the longer.

12. ROLES (See Appendix 3)

12.1 Senior Authorising officer

The senior authorising officer is the only person that can sign off a CHIS authorisation.

12.2 Authorising Officer

An Authorising Officer is a person who considers whether or not to grant an application to use directed surveillance. He/she must believe the activities to be authorised are necessary for the purposes of preventing or detecting crime and that they are proportionate to what is sought to be achieved by carrying them out.

12.3 **Senior Responsible Officer**

The Senior Responsible Officer oversees the competence of Authorising Officers and the processes in use in the council. The Senior Responsible Officer is not an Authorising Officer as it would be inappropriate to oversee his / her own authorisations. Specifically the Senior Responsible Officer will be responsible for:

- The integrity of the processes to authorise covert surveillance;
- Compliance with the statutory provisions and codes of conduct;
- Training or arranging training for Authorising Officers;
- Ensuring officers generally understand provisions relating to covert surveillance and Covert Human Intelligence Sources.
- Engagement with the Commissioners and inspectors when they conduct their inspections; and
- Overseeing the implementation of any action plans following an inspection.

12.4 **RIPA Monitoring Officer**

The RIPA Monitoring Officer has:

- The duty to maintain the list of Authorising Officers;
- The power to suspend from the list of Authorising Officers any Authorising Officer who does not follow the procedure or who does not attend training sessions; and
- The power to cancel any authorisation that is manifestly wrong.

13.0 RESPONSIBILITIES (See appendix 4)

13.1 **Chief Executive (Senior Authorising Officer)** to:

- Acts at the senior authorising officer who can sign off a CHIS authorisation

13.2 **Director of Adults and Communities (Senior Authorising Officer)** to:

- Acts at the senior authorising officer who can sign off a CHIS authorisation if person is vulnerable

13.3 **Corporate Directors** to:

- ensure all regulatory staff are aware of and trained in the Act
- delegate the task of authorising surveillance operations
- provide procedures to be adopted in the application for, granting etc of, and recording of authorisation
- ensure copies of the Codes of Practice for Covert Surveillance, The Use of Covert Human Intelligence Sources, and Acquisition and Disclosure of Communications Data are available for public reference at council offices or by post or e-mail on public request

- ensure that details of the complaints procedure involving the Investigatory Powers Tribunal are readily available for public reference purposes at council offices or by post or e-mail on public request

13.4 **Director of Legal & Governance (Senior Responsible Officer)** to:

- Fulfil the role of senior responsible officer and monitoring officer for RIPA and will be responsible for:

- the integrity of processes for the management of CHIS
- compliance with Chapter II of Part I of RIPA (acquisition and disclosure of CD)
- compliance with Part II of RIPA (surveillance and CHIS)
- oversight of the reporting of errors to the Investigatory Powers Commissioner's Office, identification of the cause(s) of errors and the implementation of processes to minimise repetition of errors
- engagement with the commissioners' inspectors when they conduct their inspections
- oversight of the implementation of post-inspection action plans approved by the commissioner.
- maintaining a log of all RIPA applications, authorisations etc including copies of all completed forms, and reviewing the quality of applications, authorisations etc.
- ensuring that all authorising officers are of an appropriate standard in light of any recommendations made by inspectors' reports
- appoint further Authorising Officers
- ensuring that cabinet members and members of the audit and governance committee have sufficient understanding of human rights and RIPA to be able to discharge their responsibilities under this policy when authorising this Policy

13.5 **Head of Legal and Deputy Monitoring Officer (Monitoring Officer)**

- maintain a record of all authorisations granted in the council
- report to audit and governance committee annually so that the committee can ensure that RIPA use is consistent with the policy and that the policy remains fit for purpose
- hold copies of all authorisations, extensions to and cancellations of authorisations and carry out an annual review of authorisations.

13.5 **Service Managers (Regulation and Technical Services) (Authorising Officer)** to:

- act as the authorising officer or for communications data the designated person to consider applications, and issue, renew, cancel or refuse authorisations relating to investigations of council employees, in accordance with the criteria set out in the Act and in the Investigatory Powers Commissioner's Office office procedures and guidance -

  https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf

- ensure applications are complete and are made out on the appropriate *pro forma*, except in the case of emergency applications

- maintain a record of applications and authorisations, and provide copies to the head of law and governance within 5 working days of the application, irrespective of whether the authorisation is granted, and copies of all cancelled authorisations within 5 working days of the cancellation.

- ensure all staff involved in surveillance operations have access to the relevant codes of practice detailed below.

- review authorisations at least monthly and record the review on the authorisation and ensure that authorisations are cancelled as soon as they have either served their original purpose or no longer meet the criteria for issue, whichever is the earlier

- in the case of communications data to act as the responsible person

13.6 **All staff involved in surveillance operations (Applying Officer)** to:

- be familiar with Act, the relevant codes of practice, and the investigatory powers commissioner's office procedures and guidance - https://www.ipco.org.uk/docs/OSC%20Procedures%20&%20Guidance%20%20%20July%202016.pdf

- ensure that the authorising officer is provided with all relevant information available to the investigation to enable an informed decision to be made

- advise the authorising officer as soon as practicable when an operation unexpectedly interferes with the privacy of an individual who is not the subject of the surveillance.

- cease the surveillance operation immediately it no longer meets the authorisation criteria

Appendix 1 to Regulation of Investigatory Powers Act 2000 (RIPA) Policy and Procedures

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

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

Investigating Officer:.....

Authorising Officer/Designated Person:.....

Officer(s) appearing before JP:.....

Address of applicant department:.....

.....

Contact telephone number:.....

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

Local authority reference:.....

Number of pages:.....

Magistrates' court:.....

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act

were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice. refuse to approve the grant or renewal of

☐ the authorisation/notice.

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

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

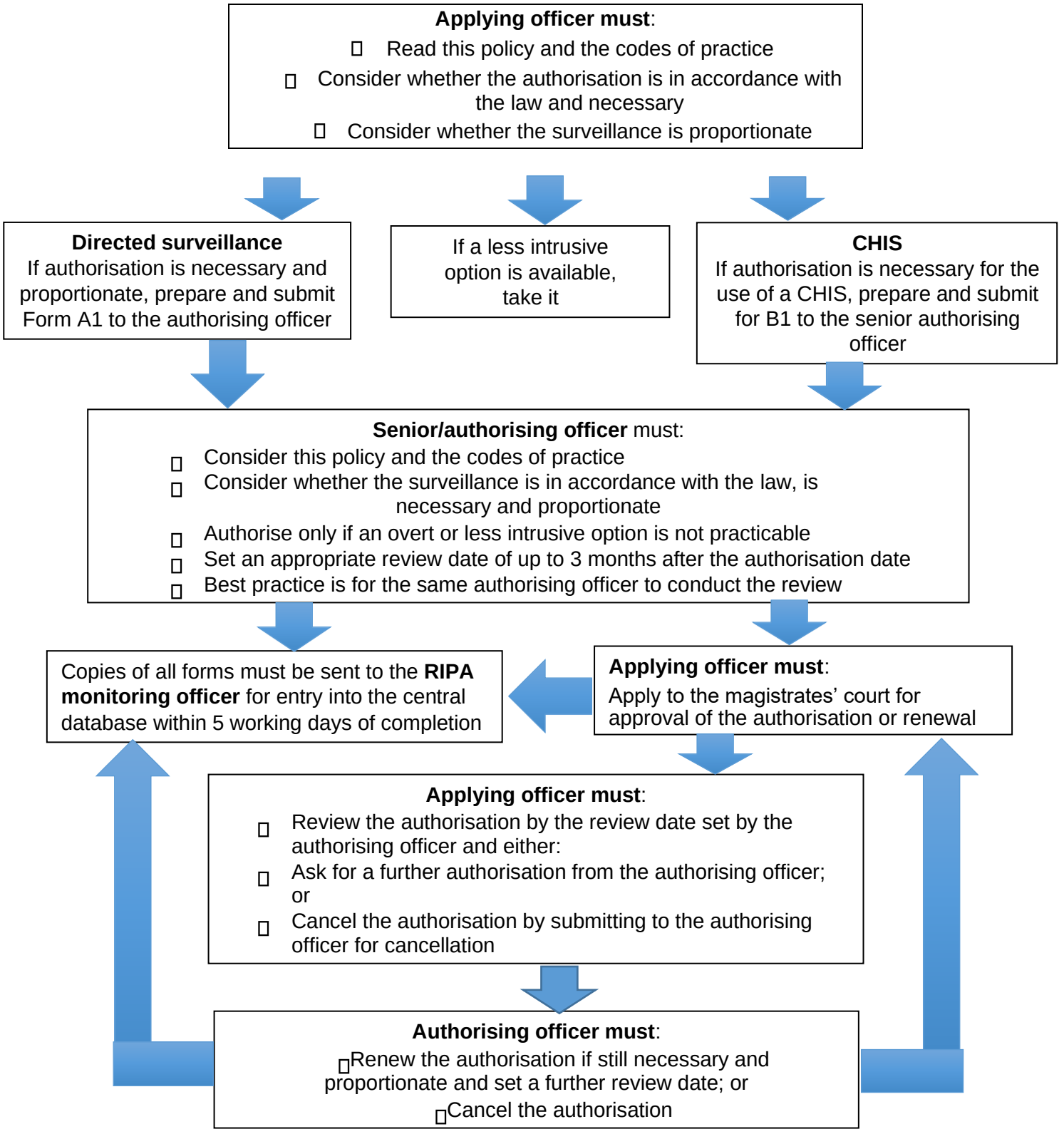
Date:

Time:

Full name:

Address of magistrates' court:

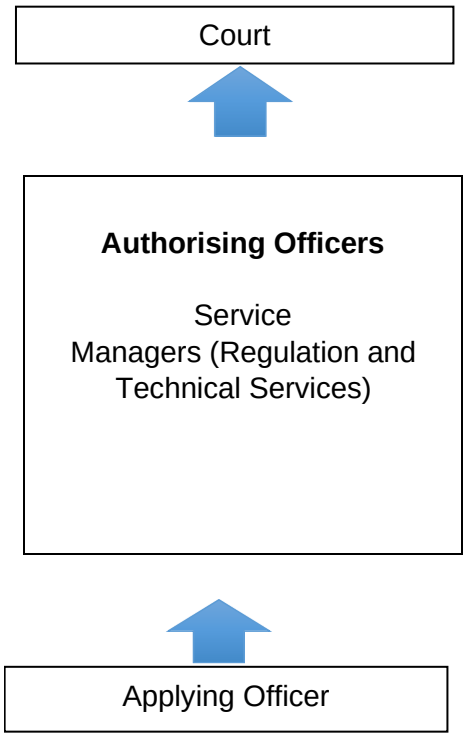
Appendix 2 - Flow Chart for Directed Surveillance and CHIS



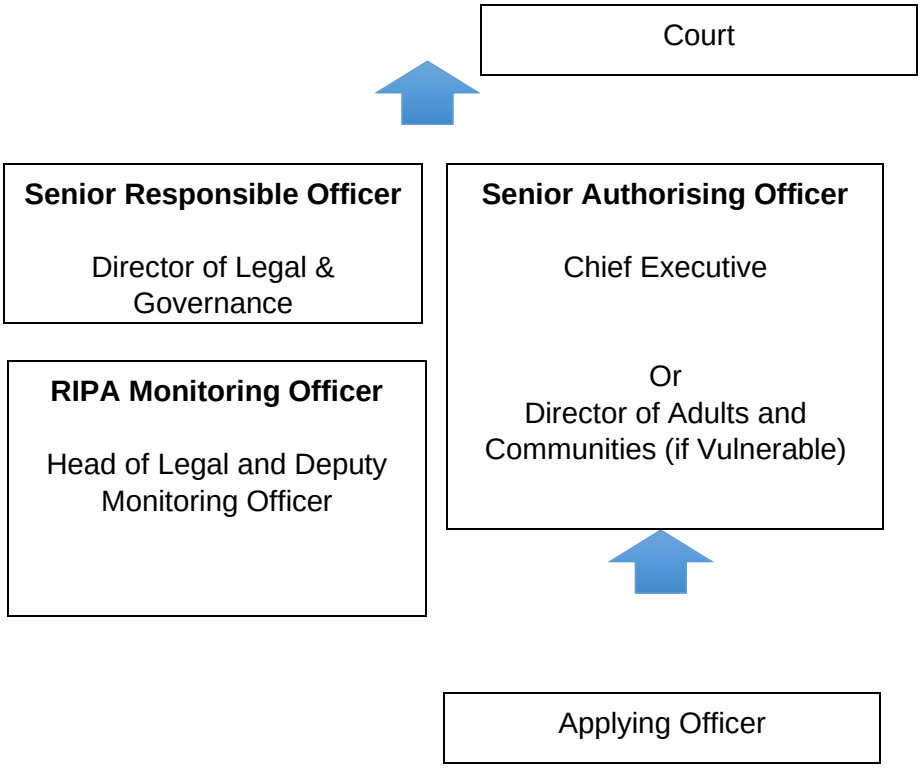
Applying officer – the person who makes a request to use RIPA powers
Authorising officer – the person who considers whether or not to grant an authorisation Senior authorising officer – the senior person who consider whether or not to grant an authorisation for the use of a CHIS

Appendix 3 - RIPA Management Structure

Directed Surveillance



CHIS



Appendix 4 - List of officer posts

Senior Responsible Officer	Director of Legal & Governance
Monitoring Officer	Head of Legal and Deputy Monitoring Officer
Senior Authorising Officer	Chief Executive or Director of Adults and Communities (if Vulnerable)
Authorising Officers	Trading Standards Service Manager Environmental Health Service Manager
Responsible person re communications data	Service Manager

Document Classification

Author Name and Role	David Hough Trading Standards Service Manager Kate Coughtrie Deputy Solicitor to the Council
Date Created	March/ April 2021
Date Issued	June 2021
Description	RIPA Policy
File Name	
Format	Microsoft Word
Geographic Coverage	Herefordshire
Master Location	Legal Services
Publisher	Herefordshire Council
Rights Copyright	Copyright of Herefordshire Council
Security Classification	
Status	
Subject	
Title	

Version Log

Version	*Status*	*Date*	*Description of Change*	*Reason For Change*
2		01 Oct 2024	Updates	Changes within council and legislation