REGULATIONS OF INVESTIGATORY POWERS ACT 2000

MARCH 2025

CORPORATE POLICY AND PROCEDURES FOR COVERT SURVEILLANCE AND THE USE OF COVERT HUMAN INTELLIGENCE SOURCES

Updated

June 2015
January 2016
November 2018
February 2019
January 2022
March 2025

THREE RIVERS DISTRICT COUNCIL

CONTENTS PAGE

Page No

NB:
The Regulation of Investigatory Powers Act 2000 ('RIPA') refers to 'Designated Officers'. For ease of understanding an application within Three Rivers DC, this Corporate Policy & Procedures Document refers to 'Authorising Officers'. Furthermore, such Officers can only act under RIPA if they have been duly authorised by the Council's Chief Executive. For the avoidance of doubt, therefore, all references to duly Authorised Officers refer to 'Designated Officers' under RIPA.

A. Introduction and Key Messages

1. This Corporate Policy & Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 ('RIPA'), The Protection of Freedoms Act 2012 and the revised Codes of Practice issued by the Home Office. 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. Any officer who is unsure about any aspect of this document should contact, at the earliest possible opportunity, the Monitoring Officer, for advice and assistance. The revised Codes of Practice can be downloaded from the Home Office web site.

2. This document and the related forms can be found on the Council's Intranet.

3. The Council will maintain, and the Monitoring Officer will check, the Corporate Register of all RIPA authorisations, reviews, renewals, cancellations and rejections. It is the responsibility of the relevant Authorising Officer, however, to place all RIPA authorisations, reviews, renewals, cancellations and rejections on the Corporate Register within 1 week of the relevant authorisation, review, renewal, cancellation or rejection.

4. Officers who; undertake surveillance, or who manage CHIS's, or who are Authorising Officers, have the responsibility of reporting to the Monitoring Officer any situations where direct surveillance or CHIS activity has been undertaken without having obtained the appropriate authority/warrant within one working day of the event having been brought to their attention. It will be the responsibility of the Monitoring Officer to investigate and to report the matter to the Investigatory Powers Commissioner no later than 10 working days from the date the event occurred.

5. RIPA, The Protections of Freedoms Act Regulations, the Codes of Practice, and this document are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This document will, therefore, be kept under review by the Monitoring Officer. Authorising Officers must bring any suggestions for continuous improvement of this document to the attention of the Monitoring Officer at the earliest possible opportunity.

6. If you are in any doubt on RIPA, the Codes of Practice, this document, or the related legislative provisions, please consult the Monitoring Officer.

7. Local authorities investigating criminal offences have powers to gain access to communications data – that is, information held by telecommunication or postal service providers about the use of their services by persons who are the subject of criminal investigations. Three Rivers DC are members of the National Anti-Fraud Network (NAFN) who will obtain such communications data on the provision of appropriate authorisation.
Communications_Data_Code_of_Practice.pdf (publishing.service.gov.uk)

8. The Council has had regard to the Codes of Practice produced by the Home Office in preparing this guidance. If any doubt arises, the Home Office Codes of Practice should be consulted. CHIS and Covert Surveillance Codes of Practice: CHIS Code draft formatted (publishing.service.gov.uk)

B. Three Rivers District Council Policy Statement

1. The Council takes seriously its statutory responsibilities under the Regulation of Investigatory Powers Act 2000, and will at all times act in accordance with the law and take necessary and proportionate action in these types of enforcement matters involving the use of covert surveillance. In that regard the Monitoring Officer is duly authorised by the Council's Leadership Team as the Council's 'Senior Responsible Officer' with responsibility to keep this Policy and Procedures document up to date and to amend, delete, add or substitute relevant provisions as necessary.

C. General Information on RIPA

1. The Human Rights Act 1998 (which incorporated the European Convention on Human Rights into UK law) requires the Council, and organisations working on its behalf, to respect the private and family life of the citizen, his/her home and his/her correspondence.

2. This is not an absolute right, but a qualified right. Accordingly, in certain circumstances, the Council, as a Relevant Public Authority under RIPA, may interfere in the citizen's right to privacy mentioned above, if such interference is: -

   (a) **in accordance with the law;**

   (a) **necessary** (as defined in this document); **and**

   (b) **proportionate** (as defined in this document).

3. Local authorities can only authorise the use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment **or** are related to the underage sale of alcohol and tobacco or nicotine inhaling products. Local authorities **cannot** authorise directed surveillance for the purpose of preventing disorder unless this involves a criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment. Local authorities are no longer able to orally authorise the use of RIPA techniques. All authorisations must be made in writing and require JP (Magistrates) approval. *(See chapter 4 para 4.42 to 4.47 of the Home Office Covert Surveillance and Property Interference Revised Code of Practice, August 2018).*

   Directed surveillance is covert surveillance that is not intrusive and is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person (other than by way of an immediate response to events or circumstances such that it is not reasonably practicable to seek authorisation under RIPA). *(See chapter E below).*
   Local authorities can only use RIPA in relation to their 'core functions' i.e., the 'specific public functions' undertaken by a particular authority in contrast to the 'ordinary functions' undertaken by all authorities (e.g. employment issues). *(See chapter E, section 15, below).*

   The internet may be used for intelligence gathering and/or as a surveillance tool. Local authority officers covertly conducting online monitoring or investigations (including Social Media) for the purpose of a specific investigation or operation which is likely to result in

the obtaining of private information about a person or group need to consider if authorisation for directed surveillance under RIPA is required, if RIPA applies.
(See chapter E, section 11, below, this includes details of when CHIS authorisation may be needed for online activity)

4. RIPA provides a statutory mechanism for authorising **covert surveillance** and the use of a **'covert human intelligence source' ('CHIS').** A CHIS is a person used by the Council to establish or maintain a personal or other relationship with another person for the covert purpose of obtaining information (e.g. undercover agents). RIPA seeks to ensure that any interference with an individual's right under the Human Rights Act 1998 is **necessary** and **proportionate**. In doing so, RIPA seeks to ensure both the public interest and the human rights of individuals are suitably balanced.

5. 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. Authorising Officers are those whose posts appear in **Appendix 1** to this document and, duly added to or substituted by the Chief Executive.

6. If the correct RIPA procedures are not followed; evidence may be disallowed by the courts, a complaint of maladministration could be made to the Ombudsman, the matter must be reported, by the Monitoring Officer, to the Investigatory Powers Commissioner, 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 document and any further guidance that may be issued, from time to time, by the Monitoring Officer.

7. A flowchart of the procedures to be followed appears at **Appendix 2**.

8. **Necessity and proportionality**

   8.1 The authorising officer must believe that the surveillance activities which are being authorised are **necessary for the purpose of preventing or detecting crime, and that the offence being investigated is one either punishable by at least 6 months imprisonment or one related to the underage sale of alcohol, tobacco or nicotine inhaling products.** This is the only statutory ground available for local authorities for the use of covert surveillance. The authorising officer must also believe that the surveillance activities are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the person who is the subject of the operation (or any other person who may be affected) against the need for the surveillance in investigative and operational terms.

   8.2 The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render intrusive actions proportionate.

8.3 The following elements of proportionality should therefore be considered:

- Balancing the size and scope of the proposed activity and the potential intrusion into the subject's personal life against the gravity and extent of the perceived crime or offence;
- Explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- Considering whether the activity is an appropriate use of RIPA and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not used.

9. **Collateral intrusion**

Before authorising applications for directed surveillance, the authorising officer should also take into account the risk of obtaining private information about persons who are not the subjects of the surveillance (members of the subject's family for example). This is referred to as collateral intrusion. All applications should include an assessment of the risk of collateral intrusion and details of any measures taken to limit this. The same proportionality tests apply to the likelihood of collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance. The authorising officer must therefore consider fully the proportionality of the proposed actions.

10. **Magistrates' Approval**

Before any authorisation for directed surveillance can be implemented the Authorising Officer must obtain the approval of a Justice of the Peace.

D. What RIPA Does and Does Not Do

1. **RIPA does**:

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

2. **RIPA does not**:

- Prejudice or dis-apply 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.

3. If the Authorising Officer or any Applicant is in any doubt, s/he should ask the Monitoring Officer BEFORE any directed surveillance and/or CHIS is authorised, renewed, cancelled or rejected.

E. Types of Surveillance

1. **'Surveillance'** includes;

   - Monitoring, observing or listening to persons, their movements, conversations, or other activities or communications, including online and social media activities.
   - Recording any information obtained in the course of authorised surveillance.
   - Surveillance, by or with, the assistance of appropriate and approved surveillance device(s).

   Surveillance can be overt or covert.

2. **Overt Surveillance**

   Most of the surveillance carried out by the Council will be done overtly – there will be nothing secretive, clandestine or hidden about it. In many cases, Officers will be behaving in the same way as a normal member of the public (e.g. in the case of most test purchases), and/or will be going about Council business openly (e.g. the Park Rangers patrolling the Parks).

3. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions, and the licensee is told that officers may visit without notice or identifying themselves to the owner/proprietor to check that the conditions are being met.

4. **Covert Surveillance**

   Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place. (Section 26(9)(a) of RIPA).

5. RIPA regulates directed surveillance, intrusive surveillance (the Council cannot carry out **intrusive surveillance**) and the use of Covert Human Intelligence Sources (CHIS).

6. **Directed Surveillance**

   Directed Surveillance is surveillance which: -

   - Is covert; and
   - Is not intrusive surveillance (see definition below – **the Council must not carry out any intrusive surveillance**);
   - Is not carried out in an immediate response to events which would otherwise make seeking authorisation under RIPA unreasonable, e.g. spotting something suspicious and continuing to observe it; and

- It is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to obtain private information** about an individual (whether or not that person is specifically targeted for purposes of an investigation). (*Section 26(10) of RIPA).*

7. **Private information**

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.

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. See section 11 below for further guidance about the use of the internet as a surveillance tool.

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.*

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.*

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.
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.

8. 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. *(Also see section 16 below).*

9. **Confidential information**

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 s/he can inform the Investigatory Powers Commissioner's Office (IPCO) or Inspector during his next inspection and the material made available to him if requested.

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.

10. For the avoidance of doubt, only those Officers, designated to be 'Authorising Officers' and identified in Appendix 1 for the purpose of RIPA, can authorise an application for 'Directed Surveillance' if, and only if, the RIPA authorisation procedures detailed in this document are followed.

Only the Chief Executive can authorise applications for covert surveillance when knowledge of confidential information is likely to be acquired.

11. **Online covert activity**

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.

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, as set out elsewhere in this code.
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).*

11.3 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 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.

11.4 As set out in paragraph 11.5 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.

11.5 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 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.

11.6 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.*

11.7 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 (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.

11.8 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.*

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.

13. **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;
- certain other specific situations (see point 17 below).

14. **Immediate response**

Covert surveillance that is likely to reveal private information about a person but is carried out by way of an immediate response to events such that it is not reasonably practicable to obtain an authorisation under RIPA.

Example: *An authorisation would not be required where Council officers conceal themselves in order to observe an incident that they happen to come across where a person appears to be in the act of illegally dumping waste.*

15. **General observation activities**

The general observation duties of Council officers do not require authorisation under the 2000 Act, whether covert or overt. Such general observation duties frequently form part of the legislative functions of the Council, as opposed to the pre-planned surveillance of a specific person or group of people. General observation duties may include monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation.

Example 1: *Intelligence suggests that a local shopkeeper is openly selling alcohol to underage customers, without any questions being asked. A trained employee or person engaged by the Council is deployed to act as a juvenile in order to make a purchase of alcohol. In these circumstances any relationship, if established at all, is likely to be so limited in regards to the requirements of the Act, that the Council may conclude that a CHIS authorisation is unnecessary. However, if the test purchaser is wearing recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a directed surveillance authorisation.*

Example 2: *Local authority officers attend a car boot sale where it is suspected that counterfeit goods are being sold, but they are not carrying out surveillance of particular individuals and their intention is, through reactive policing, to identify and tackle offenders. Again this is part of the general duties of the Council and the obtaining of private information is unlikely. A directed surveillance authorisation need not be sought.*

16. **Not related to the prevention or detection of crime punishable by 6 months imprisonment, or more, or related to the underage sale of alcohol, tobacco or nicotine inhaling products.**

In the case of local authorities directed surveillance can only be authorised under RIPA if it is for the purpose of preventing or detecting crime where the offence is punishable by a term of imprisonment of 6 months, or more, or where it is related to the underage sale of alcohol or tobacco. Covert surveillance for any other general purposes should be conducted under other relevant legislation. A local authority can only use RIPA in relation to its ‘core functions’ i.e., the ‘specific public functions’ undertaken by a particular authority in contrast to the ‘ordinary functions’ undertaken by all authorities (e.g. employment issues).

Example: *A Council employee is off work due, he claims, to an injury sustained at work for which he is suing the Council. The employee's manager suspects the employee is exaggerating the seriousness of their injury and that they are, in fact, fit enough to come to work. The manager wishes to place the employee under covert surveillance outside of his normal work environment to establish that he is indeed fit for work and to gather evidence for disciplinary proceedings against the employee for deceiving the Council. Such surveillance, even though likely to result in obtaining private information, does not constitute directed surveillance under RIPA as it does not relate to the Council's core functions. It relates instead to the carrying out of its employment functions which are common to all authorities in order to undertake surveillance of this nature the Council would need to satisfy itself that it would not be contravening the GDPR and Data Protection Act 2018 and the Council's own employment policies.*

17. **CCTV**

The use of overt CCTV cameras by the council does not normally require an authorisation under RIPA. Members of the public should be made aware that such systems are in use. For example, by virtue of cameras or signage being clearly visible, through the provision of information and by undertaking consultation. Guidance on their operation is provided in the Surveillance Camera Code of Practice issued under the Protection of Freedoms Act 2012 ("the 2012 Act") and overseen by the Surveillance Camera Commissioner. The council should also be aware of the relevant Information Commissioner's code ("In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information").

The Surveillance Camera code has relevance to overt surveillance camera systems (as defined at s29(6) of the 2012 Act) and which are operated in public places by the council. The 2012 Act places a statutory responsibility upon the council, to have regard to the provisions of the Surveillance Camera code, where surveillance is conducted overtly by means of a surveillance camera system in a public place in England and Wales.

The Surveillance Camera code sets out a framework of good practice that includes existing legal obligations, including the processing of personal data under the Data Protection Act 2018 and the councils duty to adhere to the Human Rights Act 1998.

Example: *Overt surveillance equipment, such as town centre CCTV systems, is used to gather information as part of a reactive operation (e.g. to identify individuals who have committed criminal damage after the event). Such use does not amount to covert surveillance as the equipment was overt and not subject to any covert targeting. Use in these circumstances would not require a directed surveillance authorisation.*

However, where overt CCTV or other overt surveillance cameras are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely, a record of their movements and activities) and therefore falls properly within the definition of directed surveillance. The use of the CCTV or other overt surveillance cameras in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.

Example: *A local police team receive information that an individual suspected of committing thefts from motor vehicles is known to be in a town centre area. A decision is taken to use the town centre CCTV system to conduct surveillance against that individual, such that he remains unaware that there may be any specific interest in him. This targeted, covert use of the overt town centre CCTV system to monitor and/or record that individual's movements should be considered for authorisation as directed surveillance.*

18. **Specific situations where authorisation is not available**

There are specific activities that constitute neither directed nor intrusive surveillance and therefore do not require an authorisation under RIPA. The specific situations most relevant to the Council are:

- 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. In such circumstances, whether the recording equipment is overt or covert, the member of the public knows that they are being interviewed by a Council Officer and that information gleaned through the interview has passed into the possession of the council;
- the covert recording of suspected noise nuisance's 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.

19. **<u>Examples of different types of Surveillance</u>**

Type of Surveillance	**Examples**
<u>Overt</u>	- Police Officer on patrol - Signposted Town Centre CCTV cameras (in normal use) - Recording noise coming from outside the premises after the occupier has been warned that this will occur if the noise persists. - Most test purchases (where the officer behaves no differently from a normal member of the public).
<u>Covert</u> but not requiring prior authorisation	- CCTV cameras providing general traffic, crime or public safety information
<u>Directed</u> (this is also covert) must be RIPA authorised. This includes relevant online covert activity	- Officers follow an individual or individuals over a period, to establish whether s/he is working when claiming benefit; where the offence they are investigating is punishable by a term of imprisonment of 6 months or more. - Test purchases where the officer has a hidden camera or other recording device to record information which might include information about the private life of a shop-owner, e.g. where s/he is suspected of selling alcohol or tobacco to underage customers.
<u>Intrusive</u> – **Council cannot do this!**	- Planting a listening or other device (bug) in a person's home or in their private vehicle.

F. Conduct and Use of a Covert Human Intelligence Source (CHIS)

Who is a CHIS?

1. Someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert use of the relationship to obtain information. **In normal circumstances the Council will not consider the conduct or use a CHIS.**
If consideration is given to the conduct or use of a CHIS the Monitoring Officer must be consulted first. The Council may seek the assistance of the Police to manage the CHIS.

2. The Council is not required by RIPA to seek or obtain an authorisation just because one is available (see section 80 of RIPA). The use or conduct of a CHIS, however, can be a particularly intrusive and high risk covert technique, requiring dedicated and sufficient resources, oversight and management. Authorisation is therefore advisable where the Council intends to task someone to act as a CHIS, or where it is believed an individual is acting in that capacity and it is intended to obtain information from them accordingly. The Council must ensure that all use or conduct is:
   - necessary and proportionate to the intelligence dividend that it seeks to achieve;
   - in compliance with relevant Articles of the European Convention on Human Rights (ECHR), particularly Articles 6 and 8.

3. RIPA does not apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information.

4. Three Rivers DC does not normally ask informants to gather information on the Councils behalf as this may result in the informant forming a relationship with a subject; which could result in the informant becoming a CHIS.

What must be authorised?

5. The conduct or use of a CHIS requires prior authorisation.

   - **Conduct** of a CHIS = Establishing or maintaining a personal or other relationship with a person for the covert purpose of (or is incidental to) obtaining and passing on information.

   - **Use** of a CHIS = Actions inducing, asking or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

6. **If a CHIS is used the RIPA procedures, detailed in this document, must be followed, including obtaining the approval of a Justice of the Peace.**

7. **Council Officers, and authorising officers, need to be clear that Online covert activity may also require the conduct and use of a CHIS.** ***(See chapter E, section 11, para 11.2).***

Juvenile Sources

8. Special safeguards apply to the use or conduct of juvenile sources (i.e. under 18 year olds). On no occasion can a child under 16 years of age be authorised to give information against his or her parents.

Only the Chief Executive can authorise the use of Juvenile Sources, again such authorisation must be approved by a Justice of the Peace.

Vulnerable Individuals

9. A 'vulnerable individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation.

10. A vulnerable individual will only be authorised to act as a source in the most exceptional of circumstances.

Only the Chief Executive can authorise the use of vulnerable individuals, again such authorisation must be approved by a Justice of the Peace.

Test Purchases

11. Carrying out test purchases will not (as highlighted above) require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information and, therefore, the purchaser will not normally be a CHIS. For example, authorisation would not normally be required for test purchases carried out in the ordinary course of business (e.g. walking into a shop and purchasing a product over the counter).

12. By contrast, developing a relationship with a person in the shop, to obtain information about the seller's suppliers of an illegal product (e.g. illegally imported products) will require authorisation as a CHIS. Similarly, using mobile hidden recording devices or CCTV cameras to record what is going on in the shop will require authorisation as directed surveillance. A combined authorisation can be given for a CHIS and also directed surveillance.

Anti-social behaviour activities (e.g. noise, violence, etc)

13. Persons who complain about anti-social behaviour, and are asked to keep a diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose. Recording the level of noise (e.g. the decibel level) will not normally capture private information and, therefore, does not require authorisation.

14. Recording sound (with a DAT recorder) on private premises could constitute intrusive surveillance, unless it is done overtly. For example, it will be possible to record if the noisemaker is warned (preferably in writing) that this will occur if the level of noise continues.

G. Authorising Officer Responsibilities

1. The Monitoring Officer will ensure that sufficient numbers of Authorising Officers are duly authorised to take action under this policy.

2. It will be the responsibility of Authorising Officers to ensure their relevant members of staff are suitably trained as 'Applicants' so as to avoid common mistakes appearing on forms for RIPA authorisations.

3. Authorising Officers will also ensure that staff who report to them are familiar with this policy and that they do not undertake or carry out any form of surveillance without first complying with the requirements of this document.

4. Authorising Officers must also pay particular attention to any health and safety issues that may be raised by any proposed surveillance activity. Under no circumstances, should an Authorising Officer approve any RIPA application unless, and until s/he is satisfied that a proper risk assessment has been carried out and the health and safety of Council employees/agents are suitably addressed and/or risks minimised, so far as is possible. If an Authorising Officer is in any doubt, s/he should obtain prior guidance on the same from his/her manager, the Council's Corporate Health & Safety Adviser or the Monitoring Officer.

5. Authorising Officers must obtain authorisation from a Justice of the Peace (Magistrate) before any Directed Surveillance, or the conduct or use of a CHIS, can be undertaken.

H. Authorisation Procedures

1. Directed surveillance and the use of a CHIS can only be lawfully carried out if properly authorised, and in strict accordance with the terms of the authorisation. **Appendix 2** provides a flow chart of process from application consideration to recording of information.

Authorising Officers

2. Forms can only be signed by the Authorising Officers named in **Appendix 1**.

Only the Chief Executive can authorise an application for directed surveillance when confidential information is likely to be acquired.

Appendix 1 will be kept up to date by the Monitoring Officer, and added to as needs require. If a Chief Officer wishes to add, delete or substitute a post, s/he must refer such request to the Monitoring Officer for consideration, as necessary. The Monitoring Officer is authorised to add, delete or substitute posts listed in **Appendix 1**.

3. Authorisations under RIPA are separate from delegated authority to act under the Council's Constitution. RIPA authorisations are for specific investigations only, and must be renewed or cancelled once the specific surveillance is complete or about to expire. **The authorisations do not lapse with time!**

4. The Monitoring Officer will monitor applications recorded on the central register.

Application Forms

5. Only the approved RIPA forms named in this document and found on the Council's intranet must be used.

6. **Directed Surveillance and use of Covert Human Intelligence forms.**

Form RIP 1 **Application** for Authority for Directed Surveillance
Form RIP 2 **Renewal** of Directed Surveillance Authority
Form RIP 3 **Cancellation** of Directed Surveillance
Form RIP 4 **Review** of Directed Surveillance
Form RIP 5 **Application** for use of Covert Human Intelligence Source
Form RIP 6 **Renewal** of authorisation for use of Covert Human Intelligence Source
Form RIP 7 **Cancellation** of Covert Human Intelligence Source
Form RIP 8 **Review** of use of Covert Human Intelligence Source

Grounds for Authorisation

7. Directed Surveillance (form RIP 1) can be authorised by the Council only on the following ground: -

- To prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months imprisonment **or** are related to the underage sale of alcohol and tobacco or nicotine inhaling products.

Assessing the Application Form

8. Before an Authorising Officer signs a Form, **s/he must**: -

(a) Have due regard for RIPA, the Home Office revised Codes of Practice, the Human Rights Act 1998, this Corporate Policy & Procedures Document and any other guidance issued, from time to time, by the Monitoring Officer on such matters;

(b) Satisfy his/herself that the RIPA authorisation is: -

(i) **in accordance with the law**;

(ii) **necessary** in the circumstances of the particular case on the grounds mentioned above; **and**

(iii) **proportionate** to what it seeks to achieve.

(c) 'Proportionate' means the Authorising Officer must believe that intruding upon someone's privacy through surveillance is proportionate to the desired outcome taking into account the size of the problem as against the breach of privacy

In assessing whether or not the proposed surveillance is proportionate, the Authorising Officer must be satisfied that the application form demonstrates that every other reasonable means of gathering the information has been considered and explains why the alternative means considered would not be likely to achieve the desired outcome. The Authorising Officer must also be satisfied that the proposed method of surveillance is the least intrusive.

The proportionality test is explained in more detail in Section C paragraph 8.

The Authorising Officer must in each case follow the "five Ws" (i.e, who, what, where, when and why) incorporated into the forms to make clear what is being authorised. They must also explain how and why they are satisfied that the proposed action is both **necessary** and **proportionate**. It is not enough simply to state that it is so – the reasons **why** it is so must be given.

Every question on the application form must be dealt with fully, following the prompts which are now incorporated in the forms.

(d) Take into account the risk of accidental intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid or minimise (so far as is possible) collateral intrusion and the matter may be an aspect of determining proportionality;

(e) Set a date for review of the authorisation and enter it on the Central Register. The Authorising Officer is responsible for ensuring that key dates are adhered to.

(f) Allocate a Unique Reference Number (URN) for the application as follows: - Year / Service / Number of Application

(g) Seek approval to the authorisation from a Justice of the Peace (Magistrate).

(h) Ensure that any RIPA Service Register is duly completed, and that a copy of the RIPA Forms (and any review/cancellation of the same) are recorded on the Corporate Central Register, **within 1 week of the relevant authorisation, review, renewal, cancellation or rejection**.

Additional Safeguards when Authorising a CHIS

9. When authorising the conduct or use of a CHIS, the Authorising Officer **must also: -**

(a) be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved;

(b) be satisfied that **appropriate arrangements** are in place for the management and oversight of the CHIS and this must address health and safety issues, and any risk to the CHIS arising should their role in the investigation be revealed, through a risk assessment;

(c) consider the likely degree of intrusion of all those potentially affected;

(d) consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

(e) ensure **records** containing particulars are not available except on a need to know basis.

(f) **The requirements of s.29(5) RIPA and the Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI: 2000/2725) must be considered and applied when authorising the use of a CHIS. Contact the Monitoring Officer for advice on the requirements if required.**

Duration

10. The authorisation **must be reviewed in the time stated (which can be any time stated in the application) and cancelled** once it is no longer needed. The 'authorisation' to carry out/conduct the surveillance lasts for a maximum of 3 months (from authorisation) for Directed Surveillance and 12 months (from authorisation) for a CHIS (or 4 months for a juvenile CHIS). However, whether the surveillance is carried out/conducted or not, in the relevant period, does not mean the 'authorisation' is 'spent'. In other words, **the authorisations do not expire and remain 'live' until cancelled!** The authorisations must be reviewed and/or cancelled (once they are no longer required)!

11. Authorisations can be renewed in writing before the maximum period has expired. The Authorising Officer must consider the matter afresh, including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. The Authorising Officer must still be satisfied that the surveillance is still necessary and proportionate.

12. A renewal must be approved by a JP in the same way as an original application.

I. Working With / Through Other Agencies

1. When some other agency has been instructed on behalf of the Council to undertake any action under RIPA, this document and the forms in it must be used (as per normal procedure) and the agency advised or kept informed, as necessary, of the various requirements. They must be made aware explicitly what they are authorised to do.

2. When some other agency (e.g. Police, HMRC, Home Office, etc): -

   (a) wish to use the Council's resources (e.g. CCTV surveillance systems), that agency must use its own RIPA procedures and, before any officer agrees to allow the Council's resources to be used for the other agency's purposes, s/he must obtain a copy of that agency's RIPA authorisation for the record (a copy of which must be passed to the Monitoring Officer for the Central Register) and/or relevant extracts from the same which are sufficient for the purposes of protecting the Council and the use of its resources;

   (b) wish to use the Council's premises for their own RIPA action, the officer should, normally, co-operate with the same, unless there are security or other good operational or managerial reasons as to why the Council's premises should not be used for the agency's activities. Suitable insurance or other appropriate indemnities may be sought, if necessary, from the other agency for the Council's co-operation in the agent's RIPA operation. In such cases, however, the Council's own RIPA forms should not be used as the Council is only 'assisting' not being 'involved' in the RIPA activity of the external agency.

3. In terms of 2(a), if the Police or other Agency wish to use Council resources for general surveillance, as opposed to specific RIPA operations, an appropriate letter requesting the proposed use, extent of remit, duration, who will be undertaking the general surveillance and the purpose of it must be obtained from the Police or other Agency before any Council resources are made available for the proposed use.

4. **If in doubt, please consult with the Monitoring Officer at the earliest opportunity.**

J. Record Management

1. **The Council must keep a detailed record of all authorisations, renewals, cancellations, rejections, and errors, and a Central Register of all Authorisation Forms will be maintained by the Monitoring Officer.**

2. **Records Maintained**

The following documents must be retained by the Authorising Officer for such purposes;

- a copy of the forms together with any supplementary documentation and notification of the approval given by the Authorising Officer and warrant obtained from the Magistrate; to include the date the authorisation and warrant granted and the name and job title of the authorising officer. A brief description of the investigation and the names of those being surveilled if known;
- a record of the period over which the surveillance has taken place;
- the frequency of reviews prescribed by the Authorising Officer;
- a record of the result of each review of the authorisation;
- a copy of any renewal of an authorisation and warrant obtained from the 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;
- date authorisation cancelled;
- date of any refusal to grant and authorisation;
- any errors (i.e. failures to obtain an authorisation when one was required);
- the Unique Reference Number for the authorisation (URN).

3. Each form will have a URN. The Authorising Officer will issue the relevant URN to Applicants. The cross-referencing of each URN takes place within the forms for inspection purposes. Rejected forms will also have URN's.

Central Register maintained by the Monitoring Officer

4. Authorising Officers must place details of each application on the Central Register, within 1 week of the authorisation, review, renewal, cancellation or rejection. The Monitoring Officer will monitor the same and give appropriate guidance, from time to time, or amend this document, as necessary.

5. The Council will retain records for a period of at least three years from the ending of the authorisation. The Investigatory Powers Commissioner (IPC) can inspect the Council's policies and procedures, and individual authorisations.

6. Any errors; that is failures to obtain authorisation when an authorisation should have been obtained need to be notified to the Monitoring Officer within one working day of it becoming apparent that an error has been made. They should also be logged on the central register. The Monitoring Officer will investigate and will no later than 10 working days after the error having become apparent will notify the Investigatory Powers Commissioner.

7. The Monitoring Officer will undertake a regular review of all errors and provide advice and guidance on how to avoid continuing occurrences.

Retention and Destruction of Evidence

8. Where evidence gathered from surveillance could be relevant to future or pending court proceedings, it should be retained in accordance with established disclosure requirements for a suitable period, commensurate to any subsequent review. Particular attention should be paid to the Criminal Procedure and Investigations Act 1996 which requires evidence gathered in criminal investigations to be recorded and retained.

9. All private information obtained during the course of a directed surveillance should be maintained securely and only be made available to officers entitled to view it in order to undertake their investigation, or for the purposes of conducting criminal proceedings. Officers handling private information should familiarize themselves with Home Office codes of practice on the handling of such information;
See chapter 9 of the Covert Surveillance and Property Interference Code of Practice, and chapter 8 of the Covert Human Intelligence Sources Code of Practice.
https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

K. Concluding Remarks of the Monitoring Officer

1. Where there is an interference with the right to respect for private life and family guaranteed under Article 8 of the European Convention on Human Rights, and where there is no other source of lawful authority for the interference, or if it is held not to be necessary or proportionate to the circumstances, the consequences of not obtaining or following the correct authorisation procedure set out in RIPA and this document, may be that the action (and the evidence obtained) will be held to be unlawful by the Courts pursuant to Section 6 of the Human Rights Act 1998.

2. Obtaining an authorisation under RIPA and following this document, will ensure, therefore, that the action is carried out in accordance with the law and subject to stringent safeguards against abuse of anyone's human rights.

3. Authorising Officers must exercise their minds every time they are asked to sign a form. They must never sign or rubber stamp forms without thinking about their personal and the Council's responsibilities.

4. Any boxes not needed on the form(s) must be clearly marked as being 'NOT APPLICABLE', 'N/A' or a line put through the same. Great care must also be taken to ensure accurate information is used and is inserted in the correct boxes. Reasons for any refusal of an application must also be kept on the form and the form retained for future inspections.

5. For further advice and assistance on RIPA, please contact the Council's Monitoring Officer. The Monitoring Officer will also act as Senior Responsible Officer (SRO)

Appendix 1 – List of Authorising Officer Posts

Officer
Chief Executive (only where confidential information is likely to be acquired, or where it is proposed to use juveniles or vulnerable persons as covert human intelligence sources)
Associate Director for Environment
Head of Regulatory Services
Head of Finance (Finance Shared Services)

Important Notes

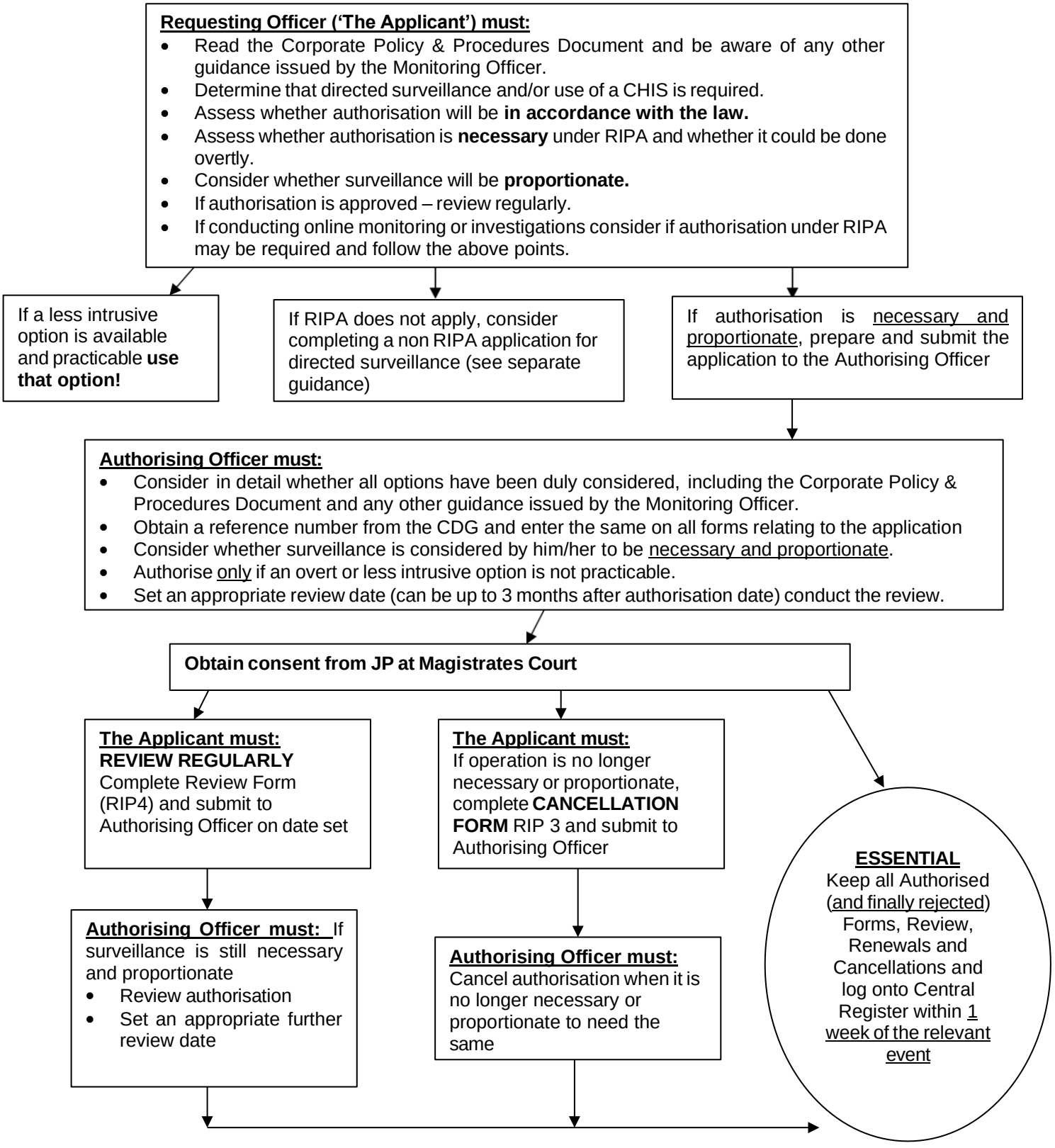
A. Only the Chief Executive is authorised to sign forms relating to Juvenile Sources and Vulnerable Individuals *(See chapter F).*

B. If the Chief Executive wishes to add, delete or substitute a post, s/he must refer such request to the Monitoring Officer for consideration, as necessary.

C. If in doubt, ask the Monitoring Officer BEFORE any directed surveillance and/or CHIS application is authorised, renewed, rejected or cancelled.

APPENDIX 2

RIPA APPLICATION FOR COVERT DIRECTED SURVEILLANCE (or use of a CHIS) FLOW CHART



NB: If in doubt, ask the Monitoring Officer BEFORE any directed surveillance, and/or CHIS, application is authorised, renewed, cancelled or rejected.

NB: Any renewal of an authoriaton will also need to go to Magistrates' Court for consent from a JP as for the original application.

THREE RIVERS
DISTRICT COUNCIL