CYNGOR SIR *POWYS* COUNTY COUNCIL.

CABINET EXECUTIVE
21st November 2023

REPORT AUTHOR:	**County Councillor Jake Berriman, Cabinet Member for a Connected Powys.**
REPORT TITLE:	**The Council's use of surveillance under the Regulation of Investigatory Powers Act 2000 2022-2023**
REPORT FOR:	**Information and decision.**

1. Purpose

1.1 To brief Cabinet on the on the council's use of covert surveillance under the Regulation of Investigatory Powers Act 200 (RIPA) for 2022-2023.

1.2 To seek approval for the revised RIPA Policy as set out in Appendix A.

1.3 To seek approval for the non-RIPA Policy and procedures as set out in Appendix B.

2. Background

2.1 RIPA provides a statutory framework regulating the use of directed surveillance and the conduct of covert human intelligence sources (informants or undercover officers) by public authorities. The Act requires public authorities, including local authorities, to use covert investigation techniques in a way that is necessary, proportionate, and compatible with human rights.

2.2 Directed surveillance is covert surveillance conducted for the purposes of a specific investigation or operation and it is likely to result in the obtaining of private information about a person. Private information includes any aspect of a person's private or personal relationship with others, including family and professional or business relationships. 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.

2.3 The Protection of Freedoms Act 2012, which requires a local authority only grant authorisations under RIPA for the use of directed surveillance where it is for the purposes of investigating criminal offences that attract a custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco.

2.4 All RIPA authorisations must be signed by an Authorising Officer. Authorising Officers must be trained before issuing any authorisations and they should attend regular refresher training. The council currently has 4 Authorising Officers.

- Professional Lead - Environmental Health (Commercial Services) & Trading Standards.
- Senior Manager - National Trading Standards Estate & Letting Agency Team.
- Principal Trading Standards Officer.
- Principal Environmental Health Officer.

2.5 A further magistrate's approval is also required before the RIPA authorisation can take effect.

2.6 Relevant Codes of Practice Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice were issued by the Home Office in 2018, and subsequently revised.

3. Investigatory Powers Commissioner's Office inspection.

3.1 The most recent inspection by the OSC, occurred in July 2022, via a desk top exercise.

3.2 An action plan to respond to the concerns of the Commissioner and implement their recommendations was developed, and recommendations inserted onto to the regulatory tracker.

3.3.1 Of the 21 actions identified,

- 18 have been completed,
- 1 is still in progress and within agreed timescales.
- 2 are over time scale, being the approval of the non-RIPA policy and procedures, which is part of this report, and the development of training on the RIPA and non-RIPA policies.

3.3.2 Of the 8 recommendations made by the Commissioner, then:

- 7 have been completed,
- 1 is still in progress and within agreed timescales.

4. Council use of RIPA.

4.1 For the financial year (1 April 2022 to 31 March 2023) the council has not undertaken any directed covert surveillance, nor has it authorised the use of a covert human intelligence source.

5. Policies.

5.1 The revised RIPA policy is attached as Appendix A. Revisions include.

- Clarification over the Council's inability to authorise Criminal Conduct by a CHIS

- Clarification over the inability of an applicant to also authorise their own applications.
- Introducing the Council's non-RIPA policy, procedures, and templates as a separate document, and subsequently removed some non-RIPA information.
- Updated CHIS Code of Practice link to new version released by the Home Office.

5.2 The newly developed non-RIPA policy and procedures is attached as Appendix B and sets out the council's position and procedures to be followed, so that any interference with an individual's right to privacy through the use of covert surveillance when RIPA authorisations are not feasible meet the requirements of the Human Rights Act 1998.

6. Resource Implications

6.1 The Council's application of RIPA is undertaken by several staff throughout the organisation, in addition to other duties.

6.2 The cost of the Council's application of and management of RIPA related activities are undertaken as part of officers' duties. No exact recordings are maintained as to time spent on RIPA related activities.

6.3 Any costs associated with RIPA activities are met from existing budgets.

6.4 The Head of Finance (Section 151 officer) notes the report.

6.5 The Head of Legal Services and Monitoring Officer is nominated as the Senior Responsible Officer.

7. Legal implications

7.1 Legal: the recommendations can be accepted from a legal point of view.

7.2 The Head of Legal Services and the Monitoring Officer has commented as follows: "I note the legal comment and approve the recommendations."

8. Climate Change & Nature Implications

8.1 NA

9. Data Protection

9.1 The Data Protection Officer is the author of this report in addition to being the RIPA Co-ordinator and has nothing further to add.

10.1. Comment from local member(s)

10.1 The use of RIPA and the appropriate policies impact with equal force across the whole County, and therefore comments have not been sought from individual Members.

11. Impact Assessment

11.1 NA

12. Recommendation

12.1 Cabinet notes that the Council has not utilised RIPA in the financial year 2022/23 and the activity undertaken in response to the Commissioner's report.

12.2 Cabinet approves the revised RIPA Policy as set out in Appendix A to the report to take immediate effect.

12.3 Cabinet approves the newly developed non-RIPA Policy and procedures as set out in Appendix B to the report to take immediate effect.

Contact Officer:	Helen Dolman
Tel:	01597 826400
Email:	helen.dolman@powys.gov.uk
Head of Service:	Diane Reynolds
Corporate Director:	Emma Palmer

Appendix A

Powys

Regulation of Investigatory Powers Act 2000 Policy
Version 2 (October 2023)

About this policy

This policy sets out the procedure to be followed by appropriate Council Staff, so that the Council's investigatory powers can be used in a lawful way. The policy relates to the use of directed surveillance, use of covert human intelligence sources (CHIS) and accessing communications data, since not all surveillance is regulated by RIPA, but all surveillance is likely to interfere with the privacy of individuals and so must be human rights compliant.

Document Control

Organisation	Powys County Council
Title	RIPA Policy
Author	Senior Manager Customer Services and Information Governance
Owner	Senior Responsible Officer – Head of Legal Services and the Monitoring Officer
Subject	Regulation of Investigatory Powers Act 2000
Protective marking	None
Review Date	October 2024

Revision History

Revision Date	Revision	Previous Version	Description of Revision
August 2022	V2	V1	Complete review
October 2023	V2.1		(1) Clarified position over inability to authorise Criminal Conduct by CHIS (2) Clarified inability of applicant to also authorise own applications (3) Introduced the Council's non-RIPA policy, procedures, and templates as separate document – removed some non-RIPA information (4) Updated CHIS Code of Practice link

1 Introduction

1.1 The Regulation of Investigatory Powers Act 2000 (the Act) and subsequent legislation (Investigatory Powers Act 2016) regulate the use of powers connected with the interception and accessing of communication data and provides a framework for the authorisation and oversight of *directed surveillance (DS)* and the use of *covert human intelligence sources (CHIS)*. The Acts were passed to ensure that law enforcement and other operations are compliant with the duties imposed on public authorities by the Human Rights Act 1998 which incorporates the rights and freedoms of the European Convention on Human Rights into our domestic law. It is unlawful for a public authority to act against a Convention right or the UK General Data Protection Regulations & Data Protection Act 2018 (DPA).

1.2 This policy and procedures document (the Policy) sets out the means of compliance with, and use of, the Act by Powys County Council (the Council) It is based upon the requirements of the Act and the Home Office's Codes of Practice on Covert Surveillance and Property Interference (August 2018), Covert Human Intelligence Sources (Aug 2018), and Communications Data (Nov 18). This version of the Policy and Guidance has been updated to take account of the changes in the Protection of Freedoms Act 2012 and SI2012/1500 "The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012

1.3. The Council has numerous statutory powers and duties to investigate activities of private individuals, groups, and organisations within its jurisdiction for the benefit and protection of the public. Such investigations may require the use of DS, CHIS and / or access to communications data. (There are many reasons why the Council might need to investigate, such as Trading Standards, licensing, audit investigation, benefit fraud, health & safety compliance, environmental health and pollution control, planning enforcement, control of building works and investigation of its own employees for the purposes of disciplinary proceedings (Core functions); this list is not intended to be exhaustive. Some of these core functions are covered by RIPA; others are not and will, therefore, not fall within the RIPA framework.

1.4 For the purposes of this policy and procedure document, surveillance is deemed to include accessing of communications data as the Council is permitted to carry out under the Act, DS and the use of a CHIS. The Act provides for the authorisation of certain investigations using such surveillance.

1.5 The Council's stated objective is compliance with the provisions of the Human Rights Act 1998, and in particular the provisions of Article 8 obliging respect for an individual's privacy. However, this is a qualified right, not an absolute one, and all investigations involve a legitimate breach of this privacy to a greater or lesser extent.

1.6. RIPA is not available to use for investigations that do not form part of the Council's core functions, and where no criminal offence is identified or where the offence identified would not be punishable by a maximum term of at least 6 months imprisonment.

1.7 This does not preclude the Council's investigators from using DS or CHIS, but if an investigation requires the use of these techniques, the investigator must apply in the same way, using the specifically developed forms, for authorisation.

1.8 The Council's non-RIPA policy, and procedures with template forms, will be followed in such cases.

1.8 **No activity must take place until Judicial Approval has been obtained.** The procedure for Judicial Approval is explained in Appendix Nine. Before undertaking surveillance and applying for Judicial Approval, the Council must be satisfied that it is undertaken either in connection with a Core Function or with a function that any ordinary employer might have (an Ordinary Function), such as the investigation of false claims for sick pay. As all surveillance is likely to intrude upon someone's human rights (for example, the right to respect for privacy and family life, home, and correspondence), it is important that the investigator is able to justify that the breach of privacy is necessary, proportionate, and lawful. It is also ESSENTIAL that the reasoning is documented, and the correct authorisations gained, in order that the Council may be held accountable for their actions.

1.9 The Council shall ensure that Officers with responsibility for authorising or carrying out surveillance or accessing communications data are aware of their obligations to comply with the Act and with the Council's policy. Furthermore, Officers shall receive appropriate training or be appropriately supervised in order to carry out functions under the Act. The list of Authorising Officers appears at Appendix One to this Document.

1.10 The Data Protection Officer shall act as the **RIPA Co-ordinator (RC)** for all applications (See Appendix Five) The Head of Legal Services and the Monitoring Officer shall discharge the duties of the **Senior Responsible Officer (SRO)**, the Council's Chief Executive shall act as the **Senior Authorising Officer (SAO),** in cases of Juvenile or Vulnerable Individual CHIS and where knowledge of confidential information is likely to be acquired.

1.11 **Failure to follow this Policy could mean that the evidence gathered may not be admissible in Court. A serious failure to adhere to the policy could be deemed as gross misconduct potentially leading to dismissal.**

2 Types of Surveillance

2.1 Surveillance includes:

- monitoring, observing, listening to persons, watching, or following their movements, listening to their conversations and other such activities or communications,
- recording anything mentioned above in the course of authorised surveillance,
- surveillance by or with the assistance of appropriate surveillance devices

Surveillance can be **overt** or **covert**.

2.2 Overt Surveillance (do not require authorisation)

2.2.1 Most of the surveillance carried out by the Council will be done ***overtly*****.** In many cases, Officers will be behaving in the same way as a normal member of the public or will be going about Council business openly (such as conducting a site visit for planning enforcement purposes)

2.2.2 Similarly, surveillance will be overt if the subject has been told that it will happen (for example, where a licensee has been made aware that officers may conduct visits without notice to check that conditions applied to a licence issued under the Licensing Act 2003 are being complied with).

The following are NOT normally Directed Surveillance:

- Activity that is observed as part of normal duties, e.g., by an officer in the course of day-to-day work.
- CCTV cameras (unless they have been directed at the request of investigators) – these are overt or incidental surveillance and are regulated by the Data Protection Act.
- Targeting a *Hot spot*, e.g., licensing officers standing on a street to monitor private hire cars plying for hire illegally where this is not part of a planned operation, or surveillance on fly tipping and dog fouling clear up. (Home Office Guidance refers.)
- Routine test purchasing of age-related products.

2.3 <u>Activity requiring authorisation.</u>

2.3.1 The following types of activity will require authorisation:

- directed surveillance.
- the conduct and use of covert human intelligence sources

2.4. Directed Surveillance

(Only when properly authorised by an Authorised Officer AND approved by a Magistrate (see Appendix 9)

2.4.1 Directed surveillance is surveillance which ~

- is covert i.e., carried out in a way that is intended to make sure that the subject of the surveillance is not aware that it is happening; and
- is not carried out in an immediate response to events which would otherwise make seeking authorisation under the Act unreasonable; and
- 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 the purposes of an investigation); and
- is not intrusive surveillance (see section 2.5 below)

2.4.2 Private Information

2.4.3 In relation to a person includes any information relating to his private and family life, his home, and his correspondence. The fact that covert surveillance occurs in a public place or on business premises does not mean that it cannot result in the obtaining of private information about a person. Prolonged surveillance targeted on a single person will undoubtedly result in the obtaining of private information about him and others that he comes into contact, or associates, with.

Expectations of Privacy:

Two people are holding a conversation on the street and, even though they are talking together in public, they do not expect their conversation to be overheard and recorded by anyone. They have a 'reasonable expectation of privacy' about the contents of that conversation, even though they are talking in the street. The contents of such a conversation should be considered as private information. A directed surveillance authorisation would therefore be appropriate for a public authority to record or listen to the conversation as part of a specific investigation or operation and otherwise than by way of an immediate response to events.

A Surveillance officer intends to record a specific person providing their name and telephone number to a shop assistant, in order to confirm their identity, as part of a criminal investigation. Although the person has disclosed these details in a public place, there is nevertheless a reasonable expectation that the details are not being recorded separately for another purpose. A directed surveillance authorisation should therefore be sought.

2.4.3 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern

of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or some cases overtly) obtained for purposes of making a permanent record on that 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 surveillance, a directed surveillance authorisation may be required.

Reconnaissance:

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. If the officers chanced to see illegal activities taking place, these could be recorded and acted upon as "an immediate response to events".

If, however, the officers intended to carry out the exercise at a specific time of day, when they expected to see unlawful activity, this would not be reconnaissance but directed surveillance, and an authorisation should be considered.

Similarly, if the officers wished to conduct a similar exercise several times, 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 or persons and a directed surveillance authorisation should be considered.

2.5 Intrusive Surveillance

2.5.1 RIPA does not authorise local authorities to carry out intrusive surveillance. Intrusive surveillance occurs when the surveillance is covert:

- relates to residential premises and private vehicles; 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.

2.5.2 Council Officers must NOT carry out intrusive surveillance:

Notes about 'Intrusive':
Surveillance is generally 'Intrusive' only if the person undertaking the surveillance is on the same premises or in the same vehicle as the subject(s) of the surveillance. Carrying out surveillance using private residential premises (with the consent of the occupier) as a 'Static Observation Point' does not make that surveillance 'Intrusive'.

A device used to enhance your external view of property is almost never an *intrusive* device. A device would only become *intrusive* where it provided a high quality of information from inside the *private residential premises*.

If premises under surveillance are known to be used for legally privileged communications, e.g., Solicitor's offices that surveillance must also be treated as *intrusive.*

Examples:
Officers intend to use an empty office to carry out surveillance on a person who lives opposite. As the office is on the 4th floor, they wish to use a long lens and binoculars so that they can correctly identify and then photograph their intended subject covertly. This is NOT *intrusive surveillance*, as the devices do not provide high quality evidence from inside the subject's premises.

Officers intend using a surveillance van parked across the street from the subject's house. They could see and identify the subject without binoculars but have realised that, if they use a 500mm lens, as the subject has no net curtains or blinds, they should be able to see documents they are reading. This IS *intrusive surveillance*, as the evidence gathered is of a high quality, from inside the premises, and is as good as could be provided by an officer or a device being on the premises.

Notes about 'Private Residential Premises' (PRP):
Premises count as PRP if they are currently used as a residence, and this includes temporary use.

Examples:
- Flats, houses, caravans etc. used as a residence are PRP.
- Hotel rooms are PRP.
- Lorry cabs and camper vans are PRP.
- Communal areas (like stairs in a block of flats) are not PRP **but**
- A stairwell in a block of flats, known to be used by a homeless person as their temporary residence **is** PRP.
- Canteens and dining areas are not PRP.
- Front gardens are not PRP.

- Setting up a local authority house for a covert operation for non-residential purposes is not PRP.

2.6 Examples of different types of surveillance

Type of Surveillance	Examples
Overt	Civil Enforcement Officer on patrol Signposted CCTV cameras (in normal use) Recording noise from outside the premises, providing that the occupier has been warned that this will take place. Enforcement Officer conducting a site visit, providing any legislative requirements as to notice have been complied with
Covert Directed	Officers following an individual over a period to establish whether they are working whilst claiming benefit.
Intrusive	Planting a listening or other device in a person's home or in their private vehicle **THE COUNCIL CANNOT AUTHORISE THIS ACTIVITY USING RIPA AND FORBIDS ITS OFFICERS FROM CARRYING OUT INTRUSIVE SURVEILLANCE.**

2.7 Duration of Directed Surveillance Authorisations / Reviews/ Renewals

2.7.1 An authorisation in writing ceases to have effect at the end of a period of 3 months beginning with the day on which it took effect being the date of authorisation by the JP. So, an authorisation starting 1 January would come to an end on 31 March.

2.7.2 Reviews - Regular reviews of authorisations should be undertaken. If, during an investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold (of at least a maximum of 6 months in prison) the use of directed surveillance should cease. The results of the review should be recorded in writing and a copy sent to the RIPA Co-Ordinator. If the surveillance provides access to confidential information or involves collateral intrusion more frequent reviews will be required. The Authorising Officer should determine how often a review should take place.

2.7.3 Renewals – While an authorisation is still effective the authorising officer can renew it if they consider this necessary for the purpose for which the authorisation was originally given. The authorisation will be renewed in writing for a further period, beginning with the day when the authorisation would have expired, but for the renewal, and can be for a further period of 3 months.

2.7.3.1 Applications requesting renewal of an authorisation are to be made on the appropriate form (Renewal Form for Directed Surveillance) links at Appendix 3 and be submitted to the Authorising Officer.

Applications for renewal will record:

- whether this is the first renewal, if not, the occasion which the authorisation has previously been renewed.
- the information as required in the original application, as it applies at the time of the renewal; together with:
    - the significant changes to the information in the previous authorisation
    - the reasons why it is necessary and proportionate to continue with the surveillance.
    - the content and value to the investigation or operation of the information so far obtained by the surveillance.
    - an estimate of the length of time the surveillance will continue to be necessary.

Renewals will also require the approval of a JP in the magistrates' court before they can take effect and investigating officers should bear in mind the relevant timescales when considering the need to renew an authorisation.

2.7.4 Cancellations - The person who granted or last renewed the authorisation MUST cancel it if they are satisfied that the directed surveillance no longer meets the criteria for authorisation. Requests for cancellation will be made on the appropriate form (Cancellation of use of surveillance) links at Appendix 3 and submitted to the authorising officer for authorisation of the cancellation.

2.7.4.1 No JP's involvement is required for cancellation. When cancelling an authorisation, the Authorising Officer should:

- record the date and times (if at all) that surveillance took place and when the order to cease the activity was made.
- the reason for cancellation
- ensure that the surveillance equipment has been removed and returned.
- provide directions for the management of the product.

- ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded.
- record the value of the surveillance or interference (i.e., whether the objectives as set in the authorisation were met).

3 USE OF COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

(Only properly authorised by an Authorised Officer AND approved by a Magistrate (see Appendix 9)

3.1.1 A CHIS is someone who establishes or maintains a personal or other relationship for the covert purpose of helping the covert uses of the relationship to obtain information.

3.1.2 RIPA does not apply to circumstances where members of the public volunteer information to the Council or to contact numbers set up to receive such information (such as a benefit fraud hotline). However, should a member of the public repeatedly provide information that might reasonably be expected to have been gained using a personal or other relationship, and should the Council intend to act upon or otherwise use this information, consideration should be given to registering the information provider as a CHIS and taking steps to secure that person's safety.

3.1.3 A relationship is covert if it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of its purpose.

3.1.4 If a person who provides information voluntarily is asked to obtain further information, it is likely that they would either become a CHIS or that Directed Surveillance authorisation should be considered.

Examples of a CHIS may include:

- Licensing Officers, working with the Police, covertly building a business relationship with a cab company which is believed to be using unlicensed drivers.

- Whistleblowing, when you actively recruit an employee to gather information on another employee who is the subject of a criminal investigation, provided this is undertaken within a formal framework (refer to the Council's Whistleblowing Policy and Procedure).

- Food Safety Officers posing as customers to get information on what is being sold at premises and developing a relationship with the shopkeeper beyond that of supplier and customer.

3.2 What must be authorised?

3.2.1 Officers must not create or use a CHIS without prior authorisation from an Authorised Officer and a Magistrate.

3.2.2 Creating (or Conduct of) a CHIS means procuring a person to establish or maintain a relationship with a person so as to secretly obtain and pass on information. The relationship could be a personal or 'other' relationship (such as a business relationship) and obtaining the information may be either the only reason for the relationship or be incidental to it. Note that it can also include asking a person to continue a relationship which they set up of their own accord.

3.2.3 Use of a CHIS includes actions inducing, asking, or assisting a person to act as a CHIS and the decision to use a CHIS in the first place.

3.2.4 Local Authorities have no power to grant the CHIS authority to commit a criminal act as part of the operation.

3.3 Test Purchases

3.3.1 A normal test purchase does not usually involve the conduct or use of a CHIS. If the test purchase does not require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information, the purchaser will not be a CHIS. In other words, if the purchaser acts in a manner entirely consistent with being an ordinary member of the public in making the test purchase, then no CHIS authorisation is needed.

3.3.2 By contrast, if a relationship is developed with the person in the shop, for example, to obtain information about supplies of goods (for example, food unfit for human consumption), then this is likely to amount to the

conduct or use of a CHIS. Similarly, if the test purchaser uses hidden devices, such as cameras or other recording devices, to record what is going on in the shop, then this will require authorisation, albeit in the form of covert directed surveillance. In some instances, a combined authorisation may be required.

3.3.3 Note that it is not just members of the public who can be a CHIS; an officer acting in this manner should be considered as a CHIS.

3.4 Use of juveniles as CHIS

3.4.1 A juvenile is a person under the age of 18. Special safeguards apply to the authorisation where the CHIS would be a child.

3.4.2 Authorisations for juvenile CHIS must not be granted unless: -

- A risk assessment has been undertaken as part of the application, covering the physical dangers and the psychological aspects of the use of the child; and
- The risk assessment has been considered by the Authorising Officer and they are satisfied that any risks identified in it have been properly explained; and
- The Authorising Officer has given particular consideration as to whether the child is to be asked to get information from a relative, guardian or any other person who has for the time being taken responsibility for the welfare of the child; and
- The Authorising Officer is satisfied that management arrangements exist which will ensure that there will always be a person who has responsibility for ensuring that an appropriate adult will be present between any meetings between Council representatives and a CHIS under 16 years of age.

3.4.3 **N.B.: A child under the age of 16 must never be asked to give information against his parents or any person who has parental responsibility for him**

3.4.4 **Authorisations for the use of a juvenile as a CHIS can only be granted by the SAO as Head of Paid Service or, in their absence, the person acting as Head of the Paid Service.**

3.4.5 The SRO will inform the Investigatory Powers Commissioner within seven working days of a juvenile CHIS authorisation.

3.5 Use of vulnerable individuals as a CHIS

3.5.1 A vulnerable individual is a person who is or maybe 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 themselves, or unable to protect themselves against significant harm or exploitation.

3.5.2 Any vulnerable individual should only be authorised to act as a CHIS in the most exceptional circumstances.

3.5.3 The SRO will inform the Investigatory Powers Commissioner within seven working days of a vulnerable individual CHIS authorisation.

3.5.3 **Authorisations for the use of a vulnerable individual as a CHIS can only be granted by the SAO as Head of Paid Service or, in their absence, the person acting as Head of the Paid Service.**

3.5.4. Additional information on the conduct or use of CHIS can be found in the Home Office Revised Code of Practice – see Appendix Three for link.

3.6 Duration of CHIS Approval

3.6.1 A written authorisation, unless renewed, will cease to have effect at the end of a period of twelve months (four months in the case of a juvenile CHIS) beginning with the day on which it took effect being the date of authorisation by the JP.

3.7 Renewals of CHIS Approvals

3.7.1 Authorisations for the conduct and use of CHIS can be renewed, the same criteria applying as on first authorisation. Applications for renewal must be made on the appropriate form and submitted to an Authorising Officer. An authorisation may be renewed more than once – provided it continues to meet the criteria for authorisation.

3.7.2 Before an Authorising Officer renews an authorisation, they must be satisfied that a review has been carried out of:

- The use made of the source during the period authorised.
- The tasks given to the source.
- The information obtained from the use or conduct of the source.

If the Authorising Officer is satisfied that the criteria necessary for the initial authorisation continue to be met, they may renew it in writing for a further period.

3.7.3 **Applications for renewal should not be made until shortly before the authorisation period is coming to an end but bearing in mind the timescales required to obtain the approval of a JP in the magistrates' court before they can take effect.**

3.8 Reviews of CHIS Approvals

3.8.1 Regular reviews of authorisations should be undertaken. The results of the review should be recorded in writing and a copy sent to the **RIPA Co-ordinator**. If the surveillance provides access to confidential information or involves collateral intrusion frequent reviews will be required. The authorising officer should determine how often a review should take place.

4 The Internet and RIPA

4.1 Nowadays investigators make much use of the internet in the course of their enquiries. Many of these enquiries are simple 'open source' enquiries and are unlikely to amount to either Directed Surveillance or the use of a Covert Human Intelligence Source. There are, however, circumstances under which RIPA authorisation may be appropriate.

4.2 Internet and RIPA **-** Normal usage

4.2.1 Where an investigator makes normal background checks on the internet, accessing pages that are in the public domain on a single occasion, this would be considered normal usage. Under these circumstances, whilst full records must obviously be kept (in order to comply with the Criminal Procedure and Investigations Act) there is no need for investigators to seek authorisation to make these enquiries. During the course of the investigation, it would be normal for an investigator to make very occasional checks on pages, in order to confirm the information contained therein or, for example, to check for changes just prior to interview.

4.2.2 If, on the other hand, investigators wish to make regular checks on pages, in order to keep check on a suspect's activities, this may amount to Directed Surveillance.

4.3 Internet and RIPA - Directed Surveillance

4.3.1 Where investigators make regular checks of a page, in order to monitor activity, this may amount to Directed Surveillance. This is because the person, whilst posting to a public forum, site, or page, may well not expect the Local Authority to be watching them.

4.3.2 An analogy must be drawn between the electronic world and the 'real' world – if investigators were to go to a public house, in order to listen to a conversation that the suspect was having, this would amount to Directed Surveillance; visiting an online forum for the same purpose is no different.

You wish to covertly watch a shop, in order to see if the shopkeeper is selling unlawful items. This is Directed Surveillance. That same shopkeeper has an online shop that you wish to check every day. What is the difference?

4.4 Internet and RIPA - Covert Human Intelligence Source (CHIS)

4.4.1 Looking at publicly available pages is normally considered 'Open Source' investigation, but the situation may change if investigators are required to *request access*, in order to view the page.

4.4.2 If investigators have to create or maintain a 'personal or other relationship' in order to access information, this could amount to becoming a CHIS if further interaction is likely to take place. A good example of this is 'Facebook', where a profile may be available for all to view ('Open Source' or Directed Surveillance) or may require investigators to send a friend request and have that request accepted.

4.4.3 An exception would be where, for example, the officer uses an identity that is manifestly overt (e.g., Powys Trading Standards) and sends the request from this identity. Under these circumstances, the viewing of the page would amount to monitoring and not Directed Surveillance or becoming a Covert Human Intelligence Source.

4.4.4 Officers are instructed to use the procedures outlined in this policy (either RIPA or Non-RIPA), if the above circumstances apply.

5 Authorisation Procedures for Directed Surveillance and CHIS.

Appendix Two provides a flow chart of the process to be followed.

5.1 Legal Advice should be sought from Legal Services prior to any application and authorisation.

5.1.1 To ensure that Directed Surveillance and the conduct or use of a CHIS can only be lawfully carried out, you must obtain legal advice from either of the following:

- Solicitor - Public Protection; or
- Professional Lead – Legal; or
- The Head of Legal Services and the Monitoring Officer.

5.2 Obtain Approval from Authorising Officers

5.2.1 DS and CHIS can only be authorised by Authorising Officers or the SAO who are named in this policy; the list of Authorising Officers appears at Appendix One. Authorising Officers will be removed from the list if they do not attend the required training programmes. Appendix one will be kept up to date by the SRO and amended as needs require, by the RIPA Co-ordinator. In addition, the SRO has authority to add, delete or substitute posts as required.

5.2.2 RIPA authorisations are for specific investigations only and must be renewed or cancelled once the specific surveillance is complete or about to expire.

5.2.3 Only the SAO can authorise the use of a CHIS who is a juvenile or vulnerable person.

5.2.4 The applicant and Authorising Officer will not be the same person, to ensure oversight of applications being made, and surveillance being undertaken.

5.4. Application Forms for Approval by Authorising Officers

5.4.1 Only the most up to date Home Office approved RIPA forms, available on the Home Office website, must be used (See Appendix three for links.) Any other forms will be rejected by the Authorising Officer and the RIPA Co-Ordinator.

5.4.2 The Authorisation Officer will check the quality of the applications made to them to ensure whether the application demonstrates sufficient grounds for authorisation.

5.4.3 The authorisation will usually be sought from the Authorising Officer associated with the service area, unless not available.

5.5 Grounds for Authorisation

5.5.1 Before considering an application for Authorisation, an Authorising Officer should be mindful of the Council's Policy and Procedures, the training provided, and any other guidance issued, from time to time, by the RIPA Co-ordinator and SRO

5.5.2 An authorisation may only be granted by an Authorising Officer where they believe from examining the Application Form that.

(a) the authorisation is necessary in the circumstances for the purpose of.

- preventing or detecting conduct which is a criminal offence being an offence punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment, or
  offences relating to the underage sale of alcohol and tobacco (being those offences listed in Article 7A of the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010/521 as amended), or
- preventing disorder where such disorder involves a criminal offence punishable (whether on summary conviction or indictment) by a maximum term of 6 months' imprisonment.

(b) the authorised surveillance is proportionate to what is sought to be achieved by it. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of

the case or if the information which is sought could reasonably be obtained by other less intrusive means. all such activity should be carefully managed to meet the objective in question

and must not be arbitrary or unfair. The least intrusive of gathering the information method will normally be considered to be the most proportionate method unless, for example, it is impractical or would undermine the investigation; and

(c) consider the risk of intrusion to the privacy of persons other than the specified subject of the surveillance (**collateral intrusion**). Measures must be taken to avoid or minimise (so far as is possible) collateral intrusion and this may be relevant to the issue of proportionality; and

(d) set a date for the review of the authorisation; and

(e) allocate a Unique Reference Number for the application as follows:

Year / Department or Operation / Number of Application; and

(f) Ensure that a copy of the RIPA form is forwarded to the RIPA Co-ordinator for entry onto the Central Register **within 48 hours of the relevant authorisation being given**.

5.5.3 NB: **The application MUST make it clear how the proposed intrusion is necessary and how an absence of this evidence would have a prejudicial effect on the outcome of the investigation. If it does not, the application MUST be refused.**

5.6.1 When completing the Authorisation Form, the Authorising Officer must expressly explain.

- Who the surveillance is directed at; and
- When and where it will take place; and
- Why the surveillance is necessary & proportionate; and
- What activities and equipment are being authorised; and
- How objectives are to be met

NB. It is not appropriate for the Authorising Officer to say, "Approved for the reason set out in the application". Each authorisation must contain the Authorising Officer's personal considerations.

5.6.2 See Appendix four for further guidance on authorisations.

Showing 'Necessity'

The application should identify the specific offence being investigated (including section and act) and the specific point(s) to prove what the proposed surveillance is intended to gather evidence about. The applicant

must show that the operation is capable of gathering that evidence and that such evidence is likely to prove that part of the offence.

5.7 Additional Safeguards when authorising a CHIS.

5.7.1 When authorising the use of a CHIS, the Authorising Officers **must also**:

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

(b) be satisfied that **appropriate arrangements** exist for the management and oversight of the CHIS; this includes health and safety issues: and

(c) consider the likely degree of intrusion of all those potentially affected, including assessing the privacy impact of the proposed surveillance and

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

(e) ensure **records** contain relevant, accurate, and appropriate information, and are not made available, except to those persons who have a need to know; and

(f) consider the additional requirements for a CHIS under the age of 18 as set out in paragraph 3.4.2 above.

5.8 Judicial Approval

5.8.1 Local Authorities **must** obtain an order approving the authorisation Directed Surveillance and / or a CHIS, before it can take effect. This order must be made by a Justice of the Peace (Magistrate). The Magistrate will consider the necessity and proportionality of the activity being proposed.

5.8.2 The procedure for obtaining Judicial approval is set out in Appendices Nine and Ten.

NB: **Since the introduction of the Protection of Freedoms Act 2012, Local Authorities no longer have powers to authorise and undertake covert activities on the basis of urgency. All authorisations must be approved a Magistrate.**

5.9 Duration of Directed Surveillance Authorisations / Reviews/ Renewals

5.9.1 **Duration -** An authorisation in writing ceases to have effect at the end of a period of 3 months beginning with the day on which it took effect being the date of authorisation by the JP. So an authorisation starting 1 January would come to an end on 31 March.

5.9.2 **Reviews -** The RIPA authorisation must be reviewed in accordance with the time stated by the Authorising Officer and cancelled once it is no longer needed. If, during an investigation it becomes clear that the activity being investigated does not amount to a criminal offence or that it would be a less serious offence that does not meet the threshold (of at least a maximum of 6 months in prison) the use of directed surveillance should cease. The results of the review should be recorded in writing and a copy sent to the RIPA Co-Ordinator. If the surveillance provides access to confidential information or involves collateral intrusion more frequent reviews will be required. The Authorising Officer should determine how often a review should take place.

5.9.3 **Renewals** –

5.9.3.1 While an authorisation is still effective the Authorising Officer can renew it if he considers this necessary for the purpose for which the authorisation was originally given. The authorisation will be renewed in writing for a further period, beginning with the day when the authorisation would have expired, but for the renewal, and can be for a further period of 3 months.

5.9.3.2 Applications requesting renewal of an authorisation are to be made on a new application and be submitted to the authorising officer with a copy being sent to the RIPA Co-Ordinator.

5.9.3.3 Applications for renewal will record:

- whether this is the first renewal, if not, the occasion which the authorisation has previously been renewed; and
- the information as required in the original application, as it applies at the time of the renewal; together with.
  - the significant changes to the information in the previous authorisation
  - the reasons why it is necessary and proportionate to continue with the surveillance.
  - the content and value to the investigation or operation of the information so far obtained by the surveillance.
  - an estimate of the length of time the surveillance will continue to be necessary.

5.9.3.4 Renewals will also require the approval of a JP in the magistrates' court before they can take effect and investigating officers should bear in mind the relevant timescales when considering the need to renew an authorisation.

5.9.3.5 Authorisations can be renewed after an Authorisation has expired but must be treated as a new application taking into accounts the benefit of the surveillance to date, and any collateral intrusion that has occurred.

To renew or not

Cases that are likely to be renewed would include the following:

- The surveillance has gathered three-quarters of the evidence required but is still crucially short of what is needed for a successful prosecution. The reason for this is that the investigator's car broke down on the last occasion.

- The surveillance has only just managed to establish a pattern of behaviour to allow for a full investigation to take place.

Cases that are unlikely to be renewed would include the following:

- The investigators have been watching the subject for the last three months and have not seen him commit the offence. They are, however, sure that they are 'at it' and would like another three months to have a look.

- Surveillance has shown that the case involves more people than originally suggested, and the surveillance operation is to be widened to gather evidence against them; In this case the extant authorisation should be cancelled, and a fresh application submitted.

5.9.4 **Cancellations**

5.9.4.1 The person who granted or last renewed the authorisation MUST cancel it if he is satisfied that the directed surveillance no longer meets the criteria for authorisation. Requests for cancellation will be made in writing and submitted to the Authorising Officer for authorisation of the cancellation. No JP's involvement is required for cancellation.

5.9.4.2 When cancelling an authorisation, the Authorising Officer should:

- record the date and times (if at all) that surveillance took place and when the order to cease the activity was made.
- the reason for cancellation
- ensure that the surveillance equipment has been removed and returned.
- provide directions for the management of the product.
- ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded.

- record the value of the surveillance or interference (i.e., whether the objectives as set in the authorisation were met).

5.10 **Confidential Information**

5.10.1 The Act does not provide any special protection for confidential information, but there are slight differences in the process. However, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy or where confidential information is involved.

5.10.2 Confidential material is anything which is:

- subject to legal privilege
- communications between a Member of Parliament and another person on constituency matters
- confidential personal information
- confidential journalistic material

5.10.3 Action which may lead to such confidential information being acquired is subject to additional safeguards.

5.10.4 Material subject to legal privilege

5.10.5 Section 98 of the Police Act 1997 describes those matters that are subject to legal privilege. Legal privilege does not apply to communications made with the intention of furthering a criminal purpose. Privilege is not, however, lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

5.10.6 Legally privileged information is particularly sensitive and surveillance which acquires such material may engage Article 6 as well as Article 8 of the Human Rights Act 1998. Legally privileged information obtained by surveillance is extremely unlikely ever to be admissible as evidence in criminal proceedings. Moreover, the fact that such surveillance has taken place may lead to related criminal proceedings being stayed as an abuse of process.

NOTE: Directed surveillance is treated for the purposes of RIPA as intrusive surveillance, where the surveillance takes place in locations where it is known that legal consultations are taking place. Local Authorities may not authorise *intrusive surveillance* using RIPA.

5.10.7 Confidential constituent information

5.10.8 Confidential constituent information is information relating to communications between a Member of Parliament and a constituent in respect of constituency matters. Such information 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.

5.10.9 Confidential Personal Information

5.10.10 Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it. This information is likely to be considered personal data, as defined by s.1 DPA, and as such is subject to protection, unless the individual is deceased.

5.10.11 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. In addition to the traditional action for breach of confidence, any misuse of this information is likely to involve a breach of the DPA, which could result in monetary penalties or criminal convictions.

5.10.12 Spiritual counselling means conversations between an individual and a minister of religion acting in his official capacity, where the individual being counselled is seeking or the minister is imparting forgiveness, absolution, or the resolution of conscience with the authority of the Divine Being(s) of their faith.

5.10.13 Confidential Journalistic Material

5.10.14 Confidential Journalistic Material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking.

5.10.15 Additional Safeguards for Confidential Information

5.10.16 An application for the use of surveillance which is likely to result in the acquisition of confidential information should only be made in exceptional and compelling circumstances. Full regard should be had to the particular proportionality issues such surveillance raises.

5.10.17 The application for authorisation should, in addition to the reasons why it is considered necessary, contain ~

- An assessment of how likely it is that confidential information will be acquired.
- Whether the purpose (or one of the purposes) of the use of surveillance or a CHIS is to obtain such confidential information

5.10.18 Additional safeguards are also to be imposed in that: -
The Authorising Officer must be the SAO or, in their absence, the person acting as SAO:

- Those involved in the surveillance must be advised that confidential material may be obtained.
- Confidential material will not be retained or copied unless there is a clear, relevant, and specific purpose for doing so.
- Confidential material will only to be disclosed to those who have a clear and substantial need to know and for a specific and proper purpose.
- Confidential material must be clearly marked as such and accompanied by a clear warning of its confidentiality.

5.10.19 **N.B.: If there is any doubt over the handling and dissemination of confidential information, advice must be sought from Legal Services *before* any dissemination of the material takes place.**

5.10.20 Where an Authorising Officer does authorise an application where confidential/legally privileged material may be obtained it will be made clear to the RIPA Co-ordinator for central records.

5.11 Covert Surveillance Equipment

5.11.1 The use of recording devices in private residential premises, after the subject of the recording (normally a nuisance neighbour) has been told they will be monitored by the use of such devices, is not surveillance, it is monitoring. (Officers must, however, be aware of the risk to health and safety of the person allowing you to use their premises.)

5.11.2 Set Up of Noise Monitoring or Recording Devices

5.11.3 Devices that make a record of noise levels are unlikely to be considered as a surveillance device, provided the guidance in this section has been followed.

5.11.4 Devices that record sound could be subject to suggestions that they are surveillance devices. The Council is clear that this is not the case, as the subject has been clearly informed that their noise levels will be monitored. Furthermore, the device is only recording noise that is clearly audible outside the monitored premises (such as in a neighbour's house or from the public highway).

5.11.5 Devices that record sound must be set so as to only record noise at the levels that are normally audible to the human ear at the location in which the device is located.

5.11.5 Devices that are not set up in accordance with the instructions in this section could be the source of complaints that they amount to unauthorised intrusive surveillance.

Officers are expressly forbidden from setting up such devices EXCEPT as set out in this section.

5.11.6 In the event that Officers wish to carry out surveillance other than monitor noise by use of surveillance devices, they must seek advice from Legal Services. The rules under which covert surveillance equipment may be installed on private premises are complex, and RIPA may not authorise the Council to act in this way.

5.11.7 Surveillance equipment will only be installed in residential premises if a member of the public has requested help or referred a complaint to the Council. Any permission to locate surveillance equipment on residential premises must be obtained in writing from the householder or tenant.

5.11.8 Surveillance devices designed or adapted for the purpose of providing information regarding the location of a vehicle alone do not necessarily constitute directed surveillance, however, the occupants of a vehicle do have privacy rights, and this would constitute directed surveillance.

5.11.9 The Council is not permitted to place a vehicle tracking device on a private vehicle for the purposes of surveillance without the owner's permission; this would constitute Property Interference.

Examples of Where Covert Surveillance Equipment Might be Used

A contractor is suspected of stealing supplies. Officers gain authorisation to observe the supply depot and to photograph any persons entering or leaving and to video any loading or unloading that takes place, using a concealed video camera.

A benefit claimant is suspected of working in a market. Officers gain authorisation to observe the market stall and to photograph the subject if they engage in trading activity, using a concealed still camera.

A person is suspected of mis-selling service to persons on the street. Officers gain authorisation to approach the man and record the conversation, using a concealed tape recorder.

5.11.10 Where the public have captured information, such as footage, screenshots, etc. then the evidence is theirs and a witness statement should be taken as to how they procured the evidence, since the integrity and provenance of the exhibit is outside of the Council's control.

5.11.11 All information captured using a surveillance device and stored within recording media used during directed surveillance or as part of the conduct of a source, whether used or unused material, must be recorded and retained and revealed to the prosecutor according to the Criminal Procedure and Investigations Act (CPIA).

5.12.1 Service Managers are responsible for ensuring that all covertly gathered material is handled and stored securely, applying relevant physical, technical, and operational security measures. Such material must be regularly reviewed to determine whether continued retention is required and justified. Where the material is no longer required then it must be securely destroyed. This is of particular importance where the material gathered is confidential or privileged information. Appendix Seven provides information as to the retention of records and material obtained.

6 Accessing Communications Data

6.1.1 The Council may only acquire communications data in relation to the "who", "when" and "where" of a communication, but not the "what" i.e., the content of what was said or written.

6.1.2 RIPA groups communications data into three types:

- "Traffic Data" which includes information about where the communications are made or received.
- "Service use information", such as the type of communication, time sent, duration.
- "Subscriber information" which includes billing information such as the name, address, and bank details of the subscriber of telephone or internet services.

6.1.3 The Council may only authorise the acquisition of the less intrusive types of communications data, i.e., service use information and subscriber information. Under no circumstances can the Council be authorised to obtain traffic data under RIPA

6.1.4 The Council is not permitted to intercept the content of any person's communications and it is an offence to do so without lawful authority.

6.1.5 The Investigatory Powers Act 2016 provides two different ways of authorising access to communications data. An Authorisation would allow the Council to **collect or retrieve** the data itself or serve a Notice to the postal or telecommunications operator which requires the operator to collect or retrieve the data and provide it to the Council. The Designated Person decides whether or not Authorisation or Notice is applied.

6.1.6 The Council is party to a collaborative agreement with the National Anti-Fraud

Network (NAFN) and uses the NAFN shared Single Point of Contact, (SPoC)
services for the acquisition of Communications Data. Applicants consult a
NAFN SPoC throughout the application process and the SPoC will scrutinise the applications independently. All applications are made electronically using the NAFN secure portal.

6.1.7 The Council therefore determines to use NAFN as its SPoC, and a subscription to NAFN services should be maintained corporately or by relevant service areas.

6.2 Applicant

6.2.1 The applicant is the person conducting an investigation or operation who makes an application in writing or electronically for the acquisition of communications data. The applicant completes an application form, setting out for consideration by the designated person, the necessity and proportionality of a specific requirement for acquiring communications data.

6.2.2 Applications, which must be retained by the Council, will:

- be made via the NAFN secure portal by completing the electronic application form.
- include the name and position held by the person making the application.
- include a unique reference number.
- include the operation name (if applicable) to which the application relates.
- specify the purpose for which the data is required, this only be for the purposes of prevention or detection of crime or of preventing disorder.
- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s), who the data relates to.
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it.
- consider and, where appropriate, describe any meaningful collateral intrusion the extent to which the privacy of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances, and identify and explain the time scale within which the data is required.

6.2.3 The applicant or Designated Officer must ensure that the SRO is aware of the application being made.

6.3 Authorising Individual

6.3.1 Communications Data can be authorised by three separate categories of individuals:

a. An Authorising Officer in the Office for Communications Data Authorisations.
b. The Designated Person who holds a prescribed office or rank in the relevant public authority. See Appendix 1
c. A judicial commissioner who is responsible for approving requests to identify or confirm journalistic sources.

6.3.2 As the Council is party to a collaborative agreement with the National Anti-Fraud Network (NAFN), then 6.3.1(a) will apply.

6.5 Designated Person

6.4.1 Designated Persons in Local Authorities can only be Directors, Head of Service, Service Manager or equivalent.

6.5 Single Point of Contact

6.5.1 The single point of contact (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 CSPs. To become accredited an individual must complete a course of training appropriate for the role of a SPoC.

6.5.2 An accredited SPoC promotes efficiency and good practice in ensuring only practical and lawful requirements for communications data are undertaken. This encourages the public authority to regulate itself. The SPoC provides objective judgement and advice to both the applicant and the designated person. In this way the SPoC provides a guardian and gatekeeper function ensuring that public authorities act in an informed and lawful manner.

6.5.3 The SPoC should be in a position to:

- assess whether the acquisition of specific communications data from a CSP is reasonably practical or whether the specific data required is inextricably linked to other data.
- advise applicants and Designated Persons on the interpretation of the Act, particularly whether an authorisation or notice is appropriate.
- provide assurance to Designated Persons those authorisations and notices are lawful under the Act and free from errors.
- provide assurance to CSPs that authorisations and notices are authentic and lawful.
- assess any cost and resource implications to both the public authority and the CSP of data requirements.

6.5.4 No application is to be submitted for authorisation until the SPoC is satisfied that it is practical and lawful and that appropriate procedures have been followed by the local authority.

7 Authorisation Procedures of Accessing Communications

7.1 The application form will be reviewed by the National Anti-Fraud Network (NAFN) SPoC.

7.1.1 When satisfied that the local authority has completed the verification process the NAFN SPoC will forward the application to the Office for Communications Data for consideration by an Authoriser.

7.1.2 An authorisation becomes valid on the date upon which the authorisation is granted. It is then valid for a maximum of one month.

7.2 Urgent Approvals

There is **NO** provision for the Council to grant urgent approvals for accessing communications data. Applications can only be made in the appropriate manner.

8 Consequences of non-compliance with this policy.

8.1 Where covert surveillance work is being proposed, this Policy and Guidance must be strictly adhered to in order to protect both the Council and individual officers from the following:

8.2. **Inadmissible Evidence and Loss of a Court Case / Employment Tribunal / Internal Disciplinary Hearing –** there is a risk that, if Covert Surveillance and Covert Human Intelligence Sources (both defined at Section 2) are not handled properly, the evidence obtained may be held to be inadmissible. Section 78 of the Police and Criminal Evidence Act 1984 allows for evidence that was gathered in a way that affects the fairness of the criminal proceedings to be excluded. The Common Law Rule of Admissibility means that the court may exclude evidence because its prejudicial effect on the person facing the evidence outweighs any probative value the evidence has (probative v prejudicial).

8.3. **Legal Challenge –** as a potential breach of Article 8 of the European Convention on Human Rights, which establishes a right to respect for private and family life, home, and correspondence, incorporated into English Law by the Human Rights Act (HRA) 1998. This could not only cause embarrassment to the Council, but any person aggrieved by the way a local authority carries out Covert Surveillance, as defined by RIPA, can apply to a Tribunal – see section 9.

8.4. **Offence of unlawful disclosure –** disclosing personal data as defined by the DPA that has been gathered as part of a surveillance operation may be an offence under Section 170 of the Act. Disclosure can be made but only where the officer disclosing is satisfied that it is necessary for the prevention and detection of crime, or apprehension or prosecution of offenders. Disclosure of personal data must be made where any statutory power or court order requires disclosure.

8.5. **Fine or Imprisonment** – Interception of communications without consent is a criminal offence punishable by fine or up to two years in prison.

8.6 **Censure** – the Investigatory Powers Commissioner's Office conducts regular audits on how local authorities implement RIPA. If it is found that a local authority is not implementing RIPA properly, then this could result in censure from the Commissioner.

8.7. **Disciplinary Action** – Failure of officers to comply with this Policy and Guidance may be a disciplinary offence under the Council's Policies and Procedures.

9 Complaints

9.1. If any person complains about matters covered by this policy, they will be directed to the Council's Complaints Procedure, and invited to use it if they wish to make a complaint regarding breach of this Policy and Guidance. ANY complaint received will be treated as serious and investigated in line with this authority's policy on complaints. **Regardless of this, the detail of an operation, or indeed its existence, must never be admitted to as part of the complaint handling process.** This does not mean it will not be investigated, just that the result of any investigation would be entirely confidential and not disclosed to the complainant.

9.2. Unlawful access or disclosure of information is likely to breach the Data Protection Act 2018, the Information Commissioner will investigate complaints and may take regulatory action.

9.3 The Investigatory Powers Tribunal is available to anyone who believes they have been victim of unlawful action by a public authority using covert investigative techniques, and or feel that their Article 8 rights have been unlawfully breached. This Tribunal is made up of senior members of the judiciary and the legal profession and is independent of the Government. The Tribunal has full powers to investigate and decide any case within its jurisdiction. Details of the relevant complaint procedure can be obtained from the following address:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

9.4 Furthermore, *Judicial Review* is available to any person who believes their rights have been unlawfully breached outside the scope of RIPA authorisation.

10 Non-RIPA Surveillance

10.1 RIPA does not grant any powers to carry out surveillance, it simply provides a framework that allows public authorities to authorise surveillance in a manner that ensures compliance with the European Convention on Human Rights.

10.2 Equally, RIPA does not prohibit surveillance from being carried out or require that surveillance may only be carried out following a successful RIPA application.

10.3 Whilst it is the intention of the Council to use RIPA in all circumstances where it is available, this is limited to preventing or detecting crime or disorder. The Council recognises that there are times when it will be necessary to carry out covert directed surveillance when RIPA is not available to use. This is known as Non-RIPA Surveillance.

10.4 In such cases the Council's non-RIPA policy and procedures will be followed.

10.5 The RIPA Co-ordinator will maintain a separate record of Non-RIPA activities.

11. Training

11.1 Relevant and appropriate training must be undertaken at regular intervals, of at least every two years by those:

- Undertaking RIPA and non-RIPA surveillance
- Making directed surveillance/CHIS/accessing communications data applications
- Authorising applications
- Acting as Designated Persons
- Acting as SRO
- Acting as RIPA Co-ordinator

11.2 Training will be given or approved by the SRO, and the RIPA Coordinator will maintain a central register of all those individuals who have undergone such training.

11.3 Authorising Officers must attend appropriate training before being permitted to authorise surveillance applications under this policy.

12 Working with Other Organisations/Agencies

12.1 Where the Council has instructed another agency to undertake any action under RIPA this must be done in accordance with the Council's policy. The appropriate Authorising Officer requesting the surveillance must ensure that the agency is made explicitly aware of the limits of the authorisation within which they can operate.

13 Duties of the Senior Responsible Officer

13.1 The Senior Responsible Officer is responsible for

- The integrity of policy and processes in place for directed surveillance/CHIS and / or accessing communications data.
- Organisational compliance with the Act(s) and Code(s) of Practice
- Reporting errors to the Investigatory Powers Commissioner, including identify causes and the implementation of process to prevent a reoccurrence.
- Engagement with the Investigatory Powers Commissioner, their inspectors, and Authorising Officers in the Office for Communications Data.
- Oversight of the implementation of post inspection recommendations and action plans, including addressing and concerns raised by inspection reports.
- Ensuring all authorising officers are of an appropriate standard.
- Informing the Investigatory Powers Commissioner of juvenile and vulnerable individual CHIS authorisations.

13.2 SRO oversight will include:

- Quarterly meetings between SRO and Authorising Officers
- RCO to inform SRO of authorisations, cancellations, and reviews.
- RCO to draw to SRO attention any authorisations not meeting section 5.6.3

14 Monitoring

14.1 The Council's Internal Audit provider shall undertake regular audits to monitor compliance with the Council's policy and RIPA legislation.

14.2 Any errors identified shall be reported directly to the SRO, who will determine whether it is a "reportable relevant error" (*S231(9) of the 2016 applies*)

14.2. The Investigatory Powers Act 2016 created the role of Investigatory Powers Commissioner to provide independent oversight of the use of investigatory powers The Commissioner will inspect Councils to assess their compliance with RIPA.

15 Oversight by Members

15.1 The Cabinet Member for a Connected Powys shall receive a report on the use of RIPA regulated activity by officers of the Council annually, and to ensure that the Policy is robust and that it is being followed by all officers involved in this area.

15.2. The report shall be produced by the RIPA Co-ordinator and presented to the Cabinet Member by the RIPA Co-ordinator and the SRO. The report must not contain any information that identifies specific persons or operations but must be clear about the nature of the operations carried out and the product obtained.

15.3 The SRO may amend this Policy and make such changes that are necessary to ensure that the policy is up to date with current legislation, without having to obtain the consent of Elected Members.

15.4. Elected Members may not inquire into individual authorisations.

APPENDIX ONE

LIST OF AUTHORISING OFFICERS

POST	NAME
Chief Executive Officer	Dr Caroline Turner (SAO)
Beverly Cadwallader	Professional Lead - Environmental Health
James Munro	Senior Manager - National Trading Standards Estate & Letting Agency Team
Jacqui Thomas	Principal Trading Standards Officer
Catherine Davies	Principal Environmental Health Officer

LIST OF DESIGNATED PERSONS FOR APPROVING THE ISSUE OF A NOTICE IN RESPECT OF ACCESS TO COMMUNICATIONS DATA

POST	NAME
Chief Executive Officer Beverly Cadwallader	Professional Lead - Environmental Health

OTHER ROLES

RIPA SRO

Head of Legal Services and the Monitoring Officer	Clive Pinney

RIPA Co-ordinator

Senior Manager Customer Services and Information Governance	Helen Dolman

IMPORTANT NOTES

A. Only the Chief Executive is authorised to sign forms relating to Juvenile Sources, Vulnerable Individuals and where knowledge of confidential information is likely to be acquired.

B. If a Director or a Head of Service wishes to add, delete, or substitute a post, he must refer such a request to the Head of Legal Services and the Monitoring Officer for consideration.

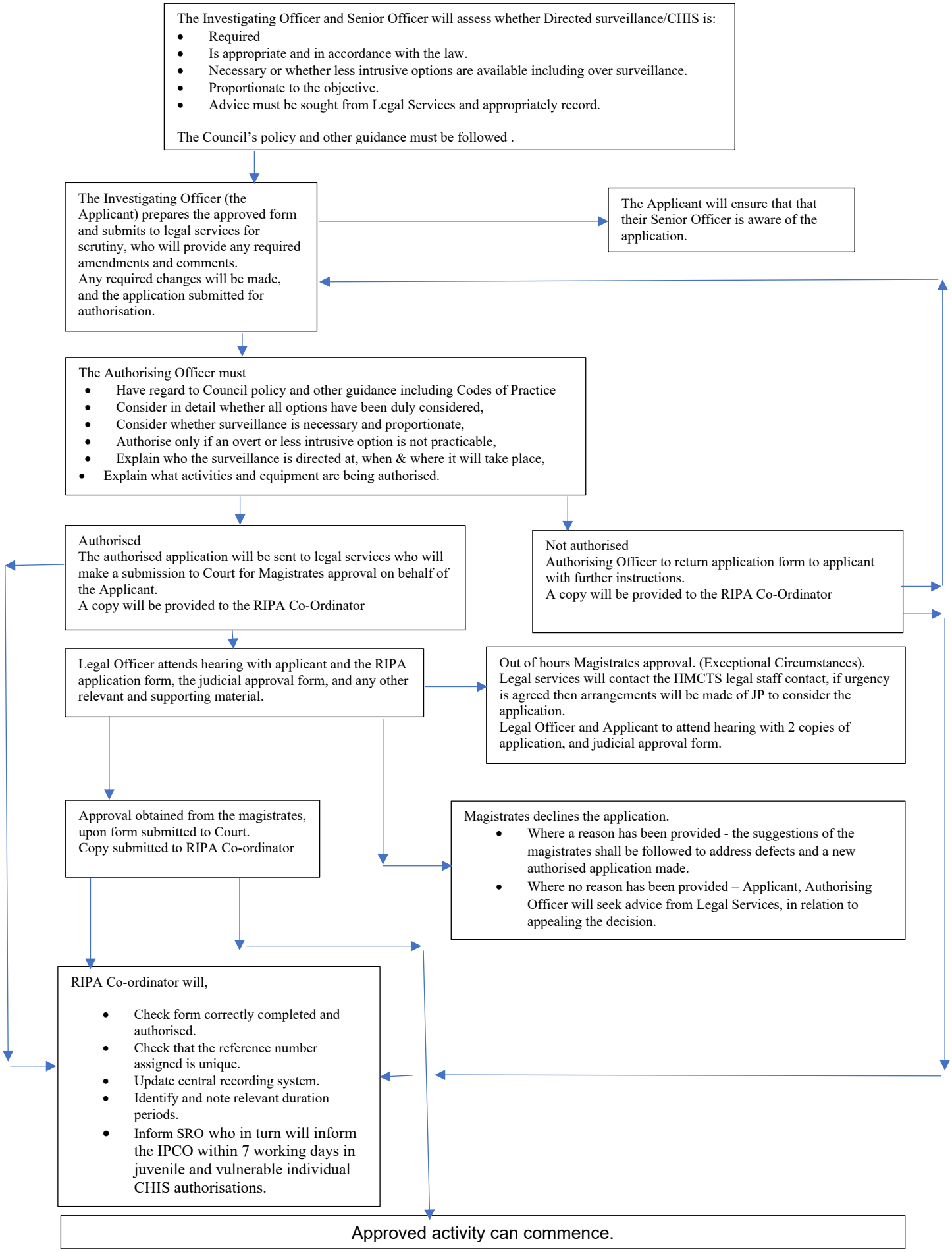
C Any Officer who is unsure about any aspect of this Policy and Procedure Document should contact, at the earliest possible opportunity, the Council's Head of Legal Services for advice and assistance.

D This Policy shall be reviewed every two years or as and when required due to changes in legislation, case law or for the better performance of the Policy. Where Authorising Officers have suggestions for continuous

improvement of this Policy these must be brought to the attention of the RIPA Co-ordinator.

APPENDIX TWO

RIPA FLOW CHART FOR DIRECTED SURVEILLANCE AND CHIS



APPENDIX THREE

RIPA Forms, Codes of Practice and Advice

The policy requires you to use the most up-to-date versions of forms and codes of practice. Rather than reproduce forms and codes of practice that are subject to change, links are provided to the currently approved versions. You should access the document you require by following the relevant link.

The most up to date RIPA forms must always be used.

The full text of the Codes of Practice is available here:

Covert Surveillance and Property Interference

Covert Human Intelligence revised Code of Practice

Communications Data

- The Acts and SIs are available here:

Regulation of Investigatory Powers Act 2000

Protection of Freedoms Act 2012

Investigatory Powers Act 2016

SI 2015 – 1500 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012

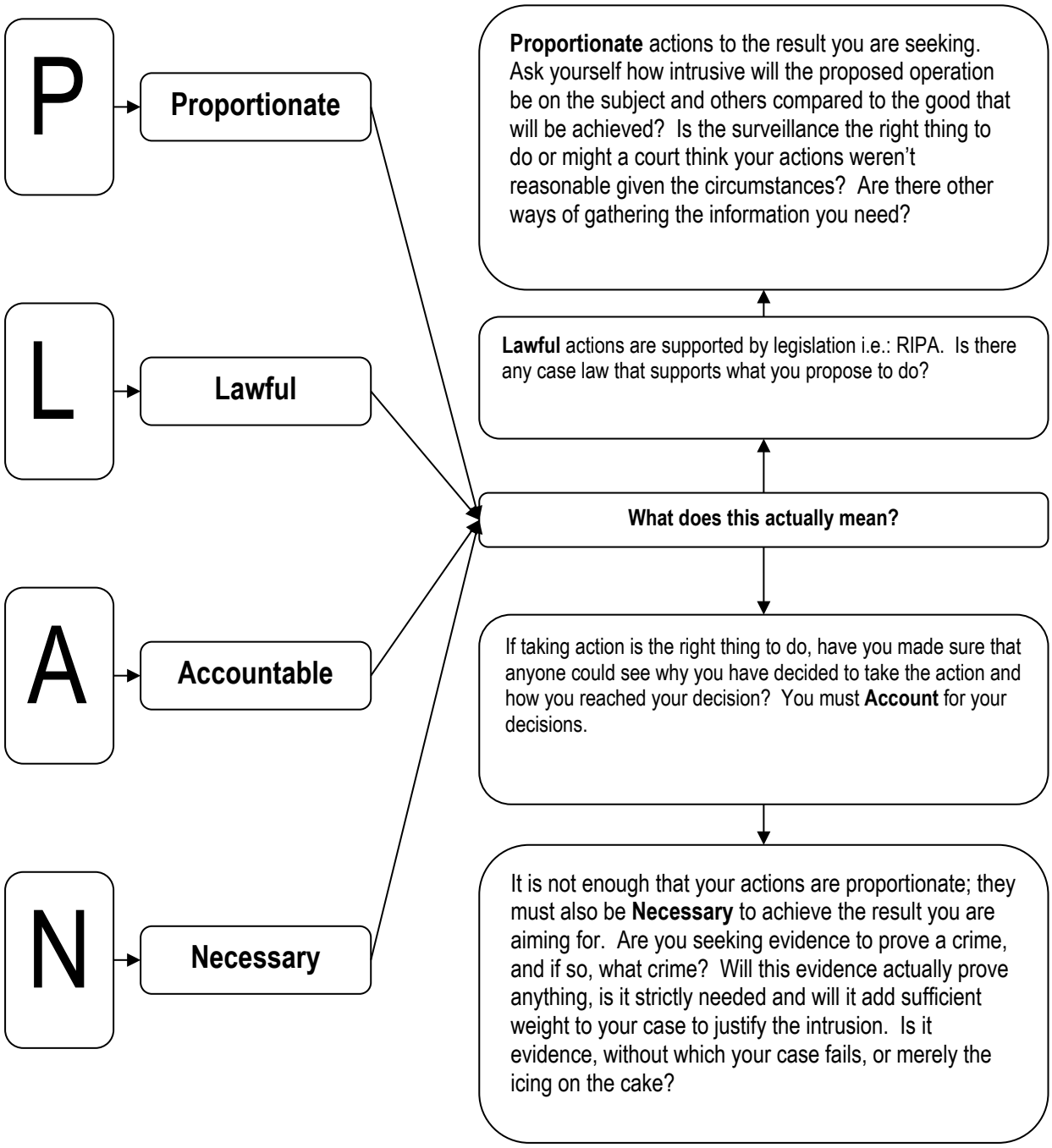
- The Investigatory Powers Commissioner's Office website has some useful information and advice and is available here:

https://www.ipco.org.uk

If you have any problems accessing these links, you must report this immediately to the RIPA Co-ordinator.

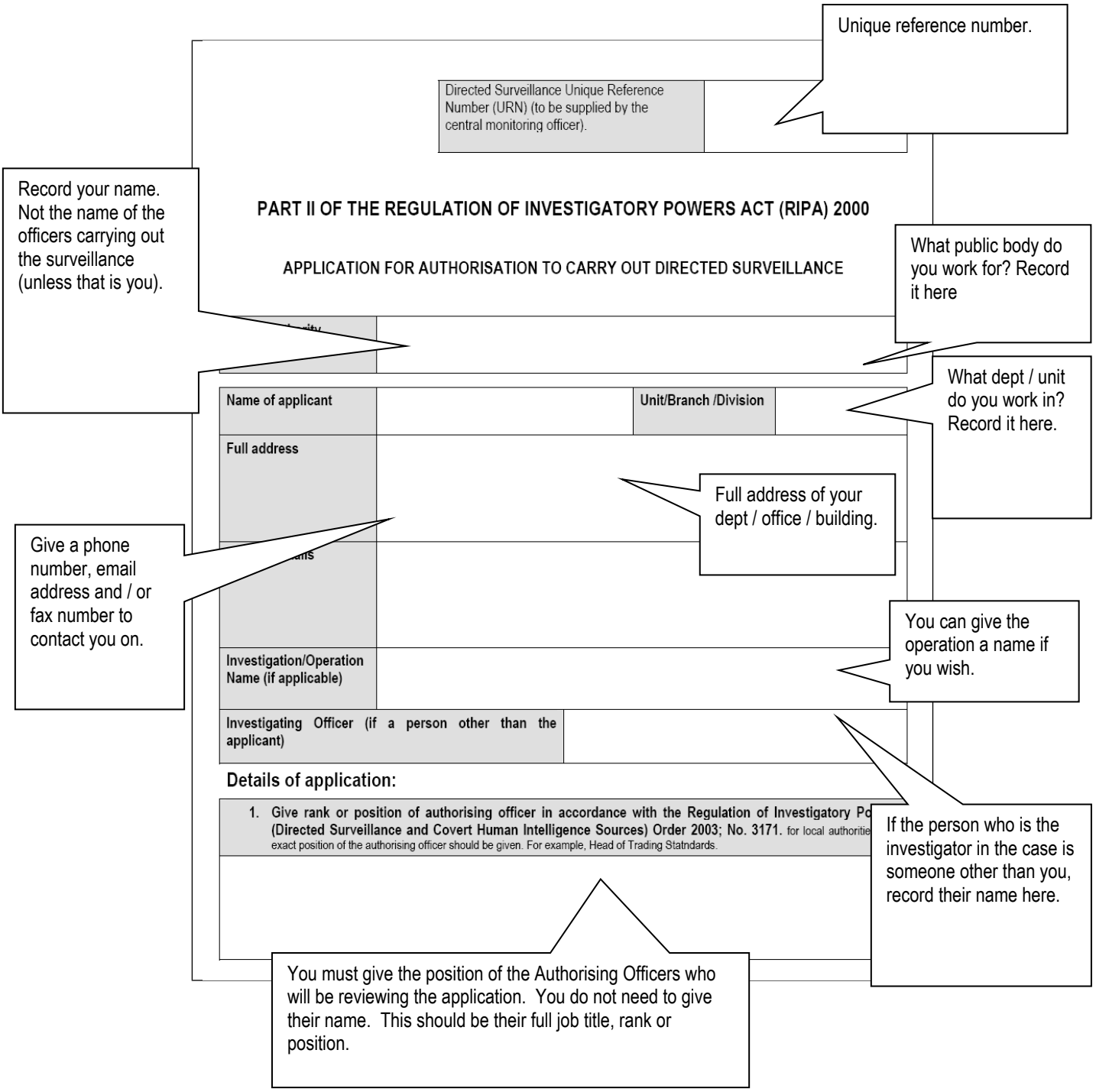
APPENDIX FOUR

Notes for Guidance for Authorisation – Directed Surveillance



APPENDIX FIVE

The RIPA 1 Form – Guidance Notes on Completion



Page Two

Enter a summary of the reason for the operation and what you are planning to do. Be brief: what will you do, why are you doing it and what will you get out of it?

2. Describe the purpose of the specific operation or investigation.

What methods will you use for the surveillance? What are the technical aspects? Who, what, when, where, how long, how many, equipment etc. Mention everything. You will not be authorised to do things you don't mention here.

3. Describe in detail the surveillance operation to be authorised and expected duration, including any premises, vehicles or equipment (e.g. camera, binoculars, recorder) that may be used.

4. The identities, where known, of those to be subject of the directed surveillance.

- Name:
- Address:
- DOB:
- Other information as appropriate:

Who are you intending to gather evidence on? If you do not know the identity of all parties you must describe them as best as you are able.

5. Explain the information that it is desired to obtain as a result of the directed surveillance.

What evidence do you intend to obtain from the surveillance? Specify exactly what you intend to get, how much and what types. This is so a judgement can be made on the weight of the evidence that you will get. Be careful what you write here: when you have achieved these aims the surveillance must stop immediately.

Page Three

6. Identify on which grounds the directed surveillance is necessary under Section 28(3) of RIPA. Delete *that are inapplicable. Ensure that you know which of these grounds you are entitled to rely on.(SI 2003 No.3171)*

- In the interests of national security;
- For the purpose of preventing or detecting crime or of preventing disorder;
- In the interests of the economic well-being of the United Kingdom;
- In the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to government department;

Cross out the conditions that do not apply to you. **In the case of a local authority, the only one that *does* is prevention or detecting crime or disorder.**

7. Explain why this directed surveillance is necessary on the grounds you have identified [Code paragraph 2.4]

Specify the offences that you are investigating or preventing. State why the information has to be obtained by surveillance, why do you need it for the reason you specified? How is it essential to the case?

8. Supply details of any potential collateral intrusion and why the intrusion is unavoidable. [Bear in mind Code paragraphs 2.6 to 2.10.]

Describe precautions you will take to minimise collateral intrusion

Collateral intrusion is where the operation interferes with the private lives of those not intended to be subject to the surveillance. This could be members of the suspect's family, their partners, colleagues or members of the public. You must identify where there is a risk that you will gather this sort of information. You must take steps to minimise this risk and show that the risk left is unavoidable: what times are you conducting surveillance? Can you avoid catching others on camera? Do you have facilities to remove identifying features? The AO must be satisfied that the need to carry out the operation outweighs this risk.

Page Four

This is where you must justify your actions as proportionate. You should have completed a planner and decided that surveillance is necessary and the last resort. Record here what you have done already and what you cannot do as it'll prejudice the investigation. Tell the AO why the need to carry out the action outweighs the suspect's right to privacy. How serious is the matter? How intrusive will the operation be on the suspect and on others? What might happen if you don't carry out surveillance? Why can't you get the information in other ways? What will be achieved by gathering the evidence?

surveillance in operational terms or can the evidence be obtained … 2.5]

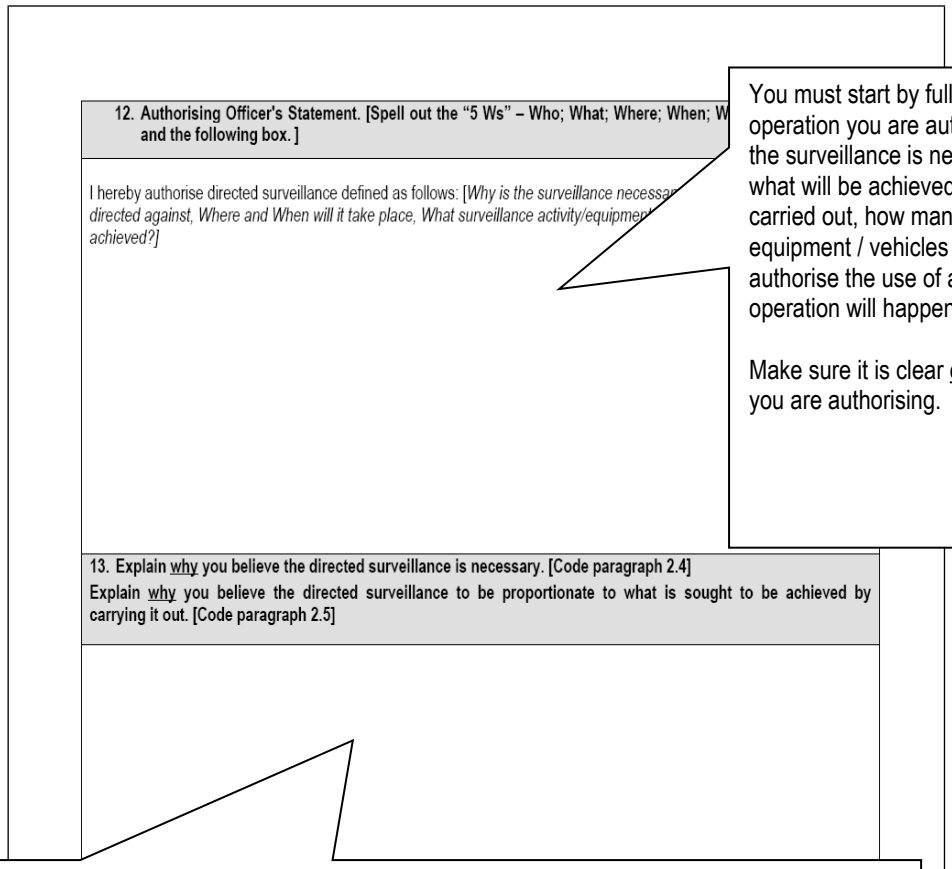
10. Confidential information [Code paragraphs 3.1 to 3.12]: INDICATE THE LIKELIHOOD OF ACQUIRING ANY CONFIDENTIAL INFORMATION:

11. Applicant's details			
Name (print)		Tel No:	
Grade/Rank		Date	
Signature			

Confidential information is *special knowledge* of a person's religious, political or medical life or information of a confidential journalistic nature (journalistic sources). Communications subject to legal privilege are also confidential. If there is a chance that you might gather this sort of information, indicate the risk here. The authorisation can then only be given by the person within your public body designated by the RIPA code of practice for this purpose.

Finish by giving your name, telephone number, job title or rank. Date the form and sign it.

Authorising Officer's Statement



You must start by fully explaining what operation you are authorising. State why the surveillance is necessary to the case, what will be achieved, how it will be carried out, how many people used, what equipment / vehicles / technology you authorise the use of and where the operation will happen.

Make sure it is clear exactly what it is that you are authorising.

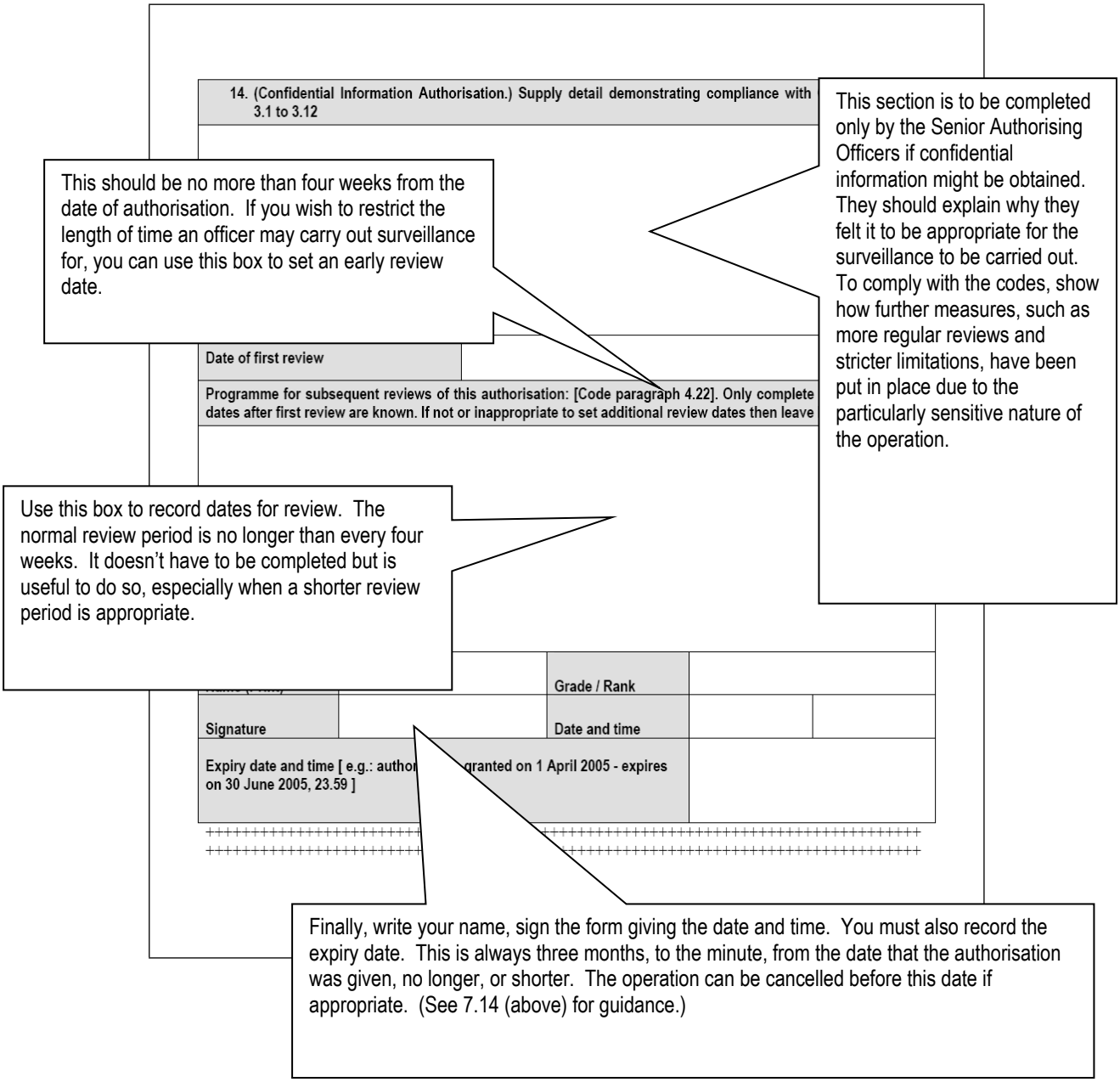
Now you must explain your decision. Simply stating that you agree with the officer who applied for the reasons they gave is not acceptable. You must give, in your own words, a detailed account of how you came to decide that the operation was necessary and proportionate. Make sure that you review the guidance in section seven and show how the evidence is necessary to the offence, and how the offence is one that it is necessary to investigate. Now ensure that you demonstrate how the officer has shown the need to obtain the evidence to be proportionate, when balanced against the person's expectation of privacy, the privacy of innocent third parties and the seriousness of the offence.

If you have completed a surveillance authorisation worksheet, go back over this as you should have already stated your reasons there.

You must explain why you feel it is in the public interest to carry out the action; is it serious, prevalent in the area, an abuse of position, premeditated? Why do you think that the investigation will be prejudiced without surveillance? Are you certain there is no other obvious and less intrusive way of obtaining the information? Does it need to be done? Record everything in this section.

This section must stand on its own, if you are called to court to justify your authorisation.

Authorising Officer's Statement



The applicant and Authorising Officer will not be the same person.

APPENDIX SIX

The Role of the RIPA Co-ordinator

The RIPA Co-ordinator will maintain a register centrally of all authorisations, grants, refusals, reviews, renewals, and cancellations.

The role of the RIPA Co-ordinator also includes:

- Reviewing decisions and raising concerns with Authorising Officers (AOs).
- Arranging training and refreshers
- Maintain the list of Designated Persons
- Updating the RIPA Policy
- Removing people from list if code not followed / training skipped etc.
- Checking for updated advice (IPCO website etc.).
- Drawing to Head of Legal Services and the Monitoring Officer's notice of potential problems.
- Produce an annual RIPA report for elected members, in line with the Covert Surveillance and Property Interference Code of Practice in order that they may review the Council's use of the legislation and ensure that policies and procedures remain fit for purpose.
- Produce annual statistic returns for the Investigatory Powers Commissioner's Office, based upon the data provided from the Authorising Officers, at such times as requested by the IPCO.

Each individual Authorising Officer is personally responsible for reporting the following information to the RIPA Co-ordinator as soon as possible and, in any event, within one working day: -

- Authorisation of DS / CHIS.
- Review of DS / CHIS.
- Renewal of DS / CHIS.
- Cancellation of DS / CHIS.
- Any unexpected deviations from normal practice or procedure.
- Any unauthorised surveillance operations.
- Any surveillance authorised outside of RIPA.
- Any other matter concerning the authorisation of surveillance that may harm the council's interests.

The RIPA Co-ordinator will keep the records for 6 years (plus the current) to comply with Home Office Guidance.

The RIPA Co-ordinator should also keep the following:

- a copy of the application, authorisation and supplementary documentation and notification of approval given by the Authorising Officers.
- a record of the period over which the surveillance has taken place.
- frequency of reviews prescribed by the Authorising Officers.
- a record of the result of each review of an authorisation.

- a copy of any renewal of an authorisation, and supporting documentation submitted when it was requested; and
- the date and time any instruction was given by the Authorising Officers.

Records must be retained in accordance with data protection legislation, and all records relating to RIPA authorisations must be kept in the strictest confidence and accessible only on a strictly need to know basis.

APPENDIX SEVEN

Retention of Authorisations and Surveillance Product.

1. The original authorisation forms must be retained on the investigation file. Copies must be retained by the RIPA Co-ordinator within the Central Monitoring Record.
2. Information will be stored securely.
3. The RIPA Co-ordinator will discuss the need to identify the retention period of the surveillance product at the time of authorisation to ensure that Information obtained through covert surveillance or property interference, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid.
4. The RIPA Co-ordinator must be sent a notification, **within 48 hours,** of all grants, refusals, reviews, cancellations, and renewals of authorisations.
5. Retention periods for records are shown in Table 1 (below)
6. Information will be destroyed securely in accordance with the retention periods set out in Table 1. The RIPA Co-ordinator must be informed when information is destroyed securely in accordance with the policy.
7. Variation to the retention periods outlined in Table 1 can be arranged through consultation and permission of the RIPA SRO.

Table 1. Retention periods

Class of record		**Retention period**
i	Central Corporate record	Permanent retention.
ii	Records of authorisations and refusals, reviews, cancellations, renewals of authorisations	Five Years
iii	Surveillance product	Deletion immediately upon identification as being no longer required for the purpose for which their collection was authorised. Surveillance product information shall be reviewed regularly, and records maintained in justification of its continued retention.
Iv	Surveillance product containing confidential or privileged material	Deletion immediately upon identification as being no longer required for the purpose for

		which their collection was authorised. Surveillance product information shall be reviewed regularly, and records maintained in justification of its continued retention

APPENDIX EIGHT

GLOSSARY

Application	A request made to an Authorising Officer to consider granting (or renewing) an authorisation for directed or intrusive surveillance (under the 2000 Act), or interference with property or wireless telegraphy (under the 1994 or 1997 Act). An application will be made by a member of a relevant public authority.
Authorisation	An application which has received the approval of an Authorising Officer. Depending on the circumstances, an authorisation may comprise a written application that has been signed by the Authorising Officer,
Authorising Officer	A person within a public authority who is entitled to grant authorisations
CHIS	Covert human intelligence sources
Confidential information	Confidential personal information (such as medical records or spiritual counselling), confidential journalistic material, confidential discussions between Members of Parliament and their constituents, or matters subject to legal privilege.
Core Functions	The statutory powers and duties given to the Council to investigate activities of private individuals, groups, and organisations within its jurisdiction for the benefit and protection of the public.
Council	Powys County Council
CSP	Communication Service Provider (a service provider that transports information electronically)
Data Protection law	The UK General Data Protection Regulation and Data Protection Act 2018.
DS	Directed surveillance.
ICD	Interception of communication data
Legal privilege	Matters subject to legal privilege are defined in section 98 of the 1997 Act. This includes certain communications between professional legal

	advisers and their clients or persons representing the client.
Officer	In this context, a person who is an employee of the Council and who has been nominated to undertake investigations that might require the use of RIPA.
Prescribed Office	Those offices, ranks and position prescribed for the purposes of section 30(1) of RIPA for the purposes of granting authorisations under sections 28 and 29 of RIPA.
Public authority	Any public organisation, agency or police force (including the military police forces).
Private information	Any information relating to a person in relation to which That person has or may have a reasonable expectation of privacy. This includes information relating to a person's private, family or professional affairs. Private information includes information about any person, not just the subject(s) of an investigation.
RIPA	Regulation of Investigatory Powers Act 2000
RC	RIPA Co-ordinator
SPoC	Single Point of Contact
SRO	Senior Responsible Officer
URN	The Unique Reference Number stating the year, division and number of each application for authorisation for directed surveillance and CHIS.

APPENDIX NINE

Procedure for Judicial Approval

Judicial Oversight

1. The *Protection of Freedoms Act* brought into law the Judicial oversight of all RIPA approvals by Local Authorities. Which means that authorisations, whilst still given by LA staff, do not take effect until a Magistrate has approved them. The Judicial oversight does not replace the authorisation process – it is an oversight function and not an authorisation function. **The Council may not undertake the regulated activity until Judicial Approval has been given.**

2. Once the application has been approved by an Authorising Officer listed in Appendix 1, the Council via Legal Services **must** apply to the Magistrates Court for an order confirming that:
    a. the person who granted or renewed the authorisation, or the notice was entitled to do so,
    b. the grant or renewal met the relevant restrictions or conditions,
    c. there were reasonable grounds for believing (at the time it was made or renewed) that obtaining the information described in the form was both necessary and proportionate; and
    d. it is still (at the time the court considers it) reasonable to believing the grant / renewal to be both necessary and proportionate.

3. The oversight will be determined at a hearing in front of a single Magistrate.

4. The Application for Judicial Approval form (See appendix Ten) must accompany all applications. The officer who made the initial application must complete this form electronically once the *Authorising Officer* has approved the application. (This also applies to requests for renewal of authorisations.)

5. The bundle for submission to the courts must include:
    a. the application for the order approving the authorisation.
    b. the authorised application or renewal form.
    c. any supporting information that, exceptionally, does not form part of the form.
    d. any information you have that might show a reason to refuse the application.
    e. an extract from the relevant legislation showing the offence being investigated and that it carries the relevant maximum sentence.

The following are things that you should normally disclose to the Court when making your application to them:

- Whether previous applications under RIPA have been rejected.
- There have been other investigations into the same subject or at the same address, regardless of whether or not they were successful.
- The proposed subject or someone living with them has alleged harassment against any person associated with the Authority.
- There have been any complaints made to the Authority by the proposed subject or anyone living with them.

N.B.: These are just examples – you must disclose anything that might influence a Magistrate in making their decision.

6. The applicant must attend the hearing and assert the accuracy of the application. They must also be prepared to answer any questions about the application and the investigation which the Magistrate may have. At the end of the application, the magistrate will give the court's decision.

7. Once the bundle has been submitted, the RIPA Co-ordinator will note this within the central record. Within 24 hours of receiving the Court's decision, the Applicant must notify the RIPA Co-ordinator and the Authorising Officer by email. The RIPA Co-ordinator must also be provided with the completed Application for Judicial Approval form, with decision of Court and detail of the Magistrate and Court. The original must be retained on the investigation file. The RIPA Co-ordinator will record the outcome within the central record.

8. In the event that the Court refuses the application, the applicant, the Authorising Officer will review the decision within 24 hours and decide if they wish to make representations to the Court before a Quashing Order is made.

9. Grounds for the submission should be set out in writing and notified to the court before the hearing. It must be drafted by the applicant and approved by the *AO*.

10. If the Authority elects to seek a hearing, the applicant, and AO will attend the hearing. At the conclusion of the hearing, the RIPA Co-ordinator will note the outcome in the central record.

APPENDIX TEN

URN	
Version	

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 28, 29 32A, 32B.

Local authority	**Powys County Council**	
Local authority department		
Offence under investigation		
Address of premises or identity of subject		
Covert technique requested	Directed Surveillance ☐	Covert Human Intelligence Source ☐

Summary of details

Investigating Officer:

Authorising Officer/Designated Person:

Officer(s) appearing before JP:

Address of applicant department:

Contact telephone number:

Contact email address (optional):

Number of pages:

Order made on an 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.

Magistrates' Court (entre name)	

Having considered the application, I (tick one):

☐ I 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

From the information provided, I grant judicial approval. The purpose of the approval is for the purpose of preventing or detecting crime under s.32 and s.28 (3)C.

Signed:

Date:

Time:

Full name:

Address of Magistrates' court:

Appendix B

Policy and Procedures into the use of non-RIPA (Regulation of Investigatory Powers Act 2000) surveillance
Version v.03 draft (October 2023)

About this policy

This policy sets out the procedure to be followed by appropriate Council Staff, so that any interference with an individual's right to privacy through the use of covert surveillance when RIPA authorisations are not applicable consider and meet the requirements of the Human Rights Act 1998.

Document Control

Organisation	Powys County Council
Title	Policy and Procedures into the use of non-RIPA (Regulation of Investigatory Powers Act 2000) surveillance
Author	Senior Manager Customer Services and Information Governance
Owner	Senior Responsible Officer – Head of Legal Services and the Monitoring
Subject	Non-RIPA surveillance
Protective marking	None
Review Date	TBC

Revision History

Revision Date	Revision	Previous Version	Description of Revision

Powys non-RIPA surveillance policy and procedures

1 Introduction

1.1 Occasionally Powys County Council authority may need to undertake covert surveillance which is not regulated by the Regulation of Investigatory Powers Act 2000 (RIPA), and thus RIPA authorisation is not feasible.

1.2 Authorisation under RIPA affords a public authority a defence However, failure to obtain an authorisation does not make covert surveillance unlawful, as indicated at section 80 of the Act and clarified by an Investigatory Powers Tribunal decision in the case of C v The Police. Simply put, covert surveillance may be undertaken outside of the RIPA authorisations regime, when the application of RIPA is not feasible.

2 Scope

2.1 This policy and procedures describe when the Council may identify a need to undertake covert surveillance, but when authorisations under RIPA are not applicable.

2.2 The Council may wish to undertake non-RIPA surveillance for the following reasons:

- Child/vulnerable adult safeguarding
- Staff malpractice
- Preventing and detecting crime that does not meet the serious crime threshold.
- Public health
- Public safety

2.3 This list is not exhaustive, and in many cases, there may be no specific crime to investigate, but a good reason to carry out the surveillance may still exist.

2.4 For this reason, Powys County Council have adopted this policy and procedures to work parallel to the RIPA policy and procedures.

3 Human Rights Compliance

3.1 Covert surveillance conducted without a RIPA authorisation will not have the protection of RIPA (i.e., the defence in section 27 of the Act).

3.2 However, covert surveillance can still be undertaken as long as it is conducted in accordance with the European Convention on Human Rights (ECHR) which is directly enforceable against public authorities pursuant to the Human Rights Act 1998.

3.3 Article 8 of the ECHR states:

“Everyone has the right to respect for his private and family life his home and his correspondence.

There shall be no interference by a public authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of public order, health or morals, or for the rights and freedoms of others."

3.4 To satisfy Article 8, the covert surveillance must be both necessary and proportionate. In deciding whether it is, the same factors need to be considered as when authorising surveillance regulated by RIPA.

3.5 These procedures ensure all activity is Human Rights compliant and that evidence of such are available for inspection by the Investigatory Powers Commissioner's Office (IPCO), as required.

4 Data protection legislation compliance

4.1 Data protection legislation will apply to the personal information to be processed, as the information will be about living individuals and will include their images, their movements, and their locations etc.

4.2 Additionally, the Information Commissioner (ICO) has produced guidance on how to undertake employee surveillance from video monitoring and vehicle tracking to email and internet surveillance, which results in compliance with data protection legislation. The Code is not law but can be taken into account by the ICO and the courts when determining if data protection legislation has been complied with.

https://ico.org.uk/media/for-organisations/documents/1064/the_employment_practices_code.pdf

(July 23 the Code is under review with consultation having taken place until January 2023)

5 Application and authorisation (See Appendix 1 for process map)

5.1 To justify the interference with an individual's right to privacy then the following must be identified:

- Legitimate reason or purpose for the covert surveillance,
- Why it is necessary,
- Why it is proportionate,

5.2 Without records being maintained the Council will struggle to defend itself against legal challenges, nor would it be possible to provide oversight to the decisions being made and establish the extent to which the rights of privacy may be being interfered with.

5.3 Previous IPCO inspection and annual reports have called for processes and documentation to be put in place for such covert surveillance.

5.4 Using the RIPA designated Authorising Officers to authorise applications will ensure decisions are made by those with Human Rights knowledge, since they will have received RIPA training.

5.5 The non-RIPA form at Appendix 2 will be used for such authorisation.

5.6 This will ensure both consistency of approach and compliance with these procedures so that this type of surveillance is only carried out where it is appropriate, necessary, and proportionate to do so.

5.7 The surveillance should cease as soon as the surveillance is no longer necessary, and a non-RIPA cancellation form should be completed. See Appendix 3

5.8 A central record of all non-RIPA authorisation, review, rejection, and cancellation forms will be maintained and monitored in a central register by the RIPA Co-ordinator for five years for oversight by the Senior Responsible Officer.

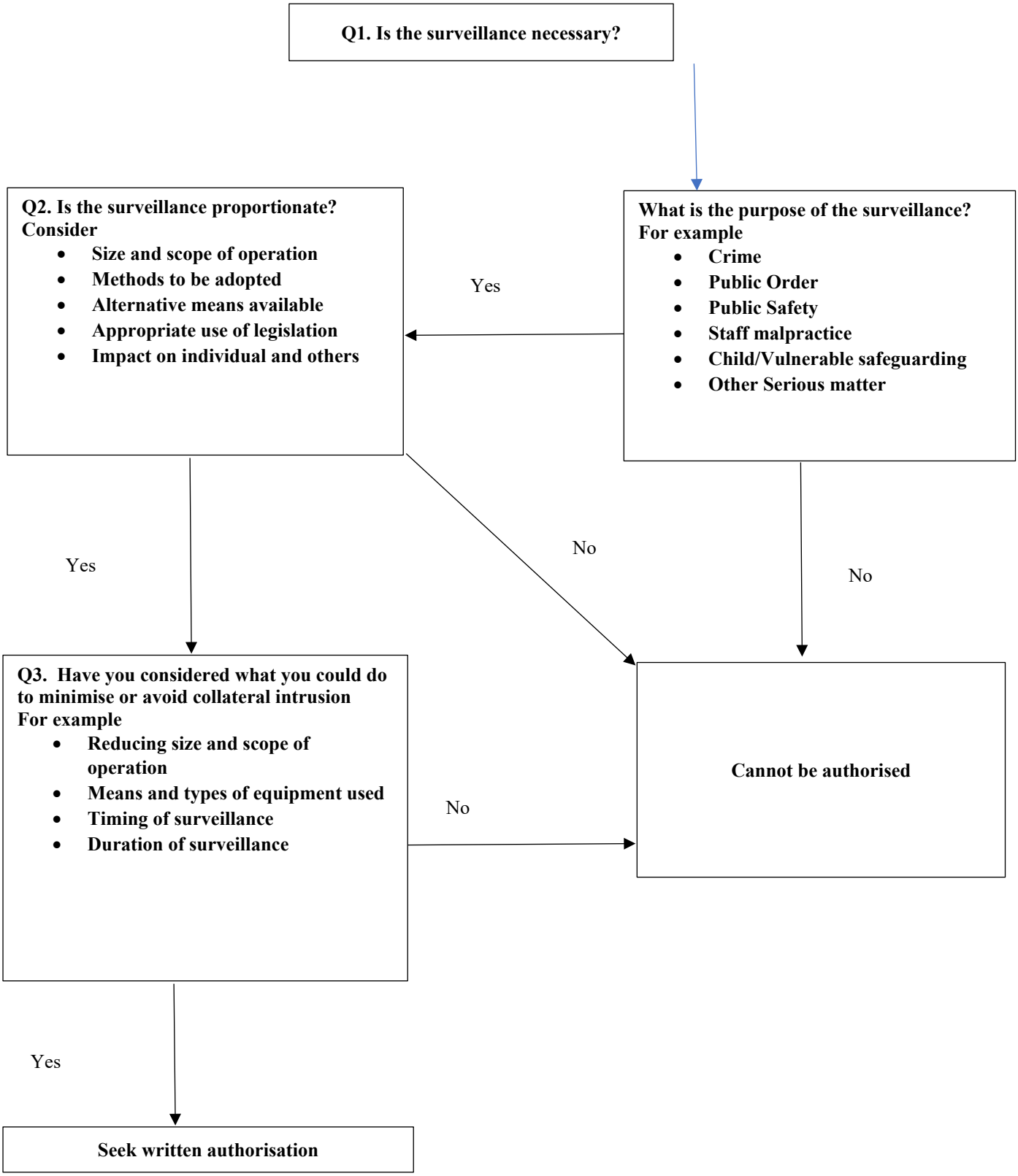
5.9 Authorising Officers will send completed forms to the RIPA Co-ordinator

5.10 The Senior Responsible Officer (SRO) for RIPA, will include these authorised Non-RIPA forms in their RIPA oversight activities, in line with Section 13 of the Council's RIPA policy.

5.11 If the Council authorises a non-employee (e.g., an enquiry agent) to conduct covert surveillance then that person/company is acting as an agent for the Council. The Authorising Officer must ensure that the person/company is competent, and they have provided a written acknowledgment that they are an agent of the Council and will comply with the authorisation, with relevant data protection agreements being in place.

Appendix 1

Process map - Authorising non-RIPA Surveillance



Appendix 2

Unique Reference Number (URN)	

Powys County Council

Non-RIPA Surveillance Form

NB *This form is only to be used in circumstances when an authorisation under the Regulation of Investigatory Powers Act 2000 is not available under the legislation or where it is considered that such an authorisation is not required.*

Public Authority **(Including full address)**	Powys County Council County Hall Llandrindod Wells Powys LD1 5LG

Name of Applicant		**Section or Team**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			
Investigating Officer (if a person(s) other than the applicant)			

Identify why a RIPA authorisation is not available under the legislation or it is considered that a RIPA authorisation is not required

Details of application:

1. Give rank or position of Authorising Officer

Outline the nature of the matter and how surveillance will contribute to the investigative strategy at this stage

2. Describe the purpose of the investigation / activity and include the operation number (if applicable).

3. Describe in detail the activity to be authorised and expected duration, including any premises, vehicles or equipment (e.g., camera, binoculars, recorder) that may be used.

4. The identities of those to be subject of the activity, where known.

Include name and address

5. Detail the information that the activity hopes to achieve.

Explain why it is considered that surveillance is necessary i.e., because there are no other alternative overt means of checking the situation, or is the surveillance is considered necessary to ascertain the veracity of information?

6. Explain <u>why</u> this activity is necessary

7. Explain <u>why</u> this activity is proportionate to what it seeks to achieve.

How intrusive might it be on the subject or on others? And why is this intrusion outweighed by the need for the activity in operational terms or can the evidence be obtained by any other means?

8. Explain <u>why</u> this activity is non discriminatory

9. Supply details of any potential collateral intrusion and why the intrusion is unavoidable.

Consider the age of individuals. Whether children are involved

Describe precautions you will take to minimise collateral intrusion

Indicate the likelihood of acquiring any confidential information

10. Confidential information.

11. Applicant's Details			
Name		**Tel No:**	
Grade/Rank		**Date**	
Signature			

12. Authorising Officer's statement.				
Date of first review		.		
Name (Print)		**Grade/Rank**		
Signature		**Date and time**		

Spell out the "5 Ws" – Who; What; Where; When; Why and How & how the activity is deemed necessary and proportionate

Appendix 3

Unique Reference Number (URN)	

Cancellation of a non-RIPA surveillance authorisation

Public Authority *(Including full address)*	Powys County Council County Hall Llandrindod Wells Powys LD1 5LG

Name of Applicant		**Section or Team**	
Full Address			
Contact Details			
Investigation/Operation Name (if applicable)			

Details of cancellation:

1. Explain the reason(s) for the cancellation of the authorisation:

2. Explain the value of surveillance in the operation:

3. Authorising Officer's statement.			
I, [insert name], hereby authorise the cancellation of the directed surveillance investigation/operation as detailed above.			
Name (Print)	----------	**Grade**	----------
Signature	----------	**Date**	----------

4. Time and Date of when the Authorising Officer instructed the surveillance to cease.			
Date:		**Time:**	

5. Authorisation cancelled.	**Date:**	**Time:**