APPENDIX

CAERPHILLY COUNTY BOROUGH COUNCIL

POLICY, PROCEDURES & FORMS

On

DIRECTED SURVEILLANCE

And use of

COVERT HUMAN INTELLIGENCE SOURCES

Under the

REGULATION OF INVESTIGATORY POWERS ACT 2000

As amended by The Protection of Freedoms Act 2012

Amended September 2015

APPENDIX

CONTENTS

Appendix 1

Flow chart of Procedure

Appendix 2

Details of Authorising Officers

Appendix 3

Forms

Part A RIPA Forms
Part B Human Rights Act 1998 – Additional Forms

NOTE:

This document must be read in conjunction with the Regulation of Investigatory Powers Act Codes of Practice issued by the Home Office on:

- **Covert Surveillance & Property Interference 2014**
- **Covert Human Intelligence Sources 2014**
- **Acquisition and Disclosure of Communications Data ('Comms COP')**

And in respect of CCTV

- **The Information Commissioner's CCTV Code of Practice ('ICO CoP')**

This document must also be read in conjunction with the Procedures and Guidance issued by the Office of Surveillance Commissioners (December 2014).

Copies of this document, application forms, Code of Practice and the Central Register of Trained Officers are maintained by Legal Services.

APPENDIX

CAERPHILLY COUNTY BOROUGH COUNCIL
POLICY & PROCEDURES
REGULATION OF INVETIGATORY POWERS ACT 2000 (RIPA)

A. Introduction & Key Messages

1. This Corporate Policy & Procedures Document is based upon the requirements of The Regulation of Investigatory Powers Act 2000 (RIPA) and Home Office's Code of Practices on "Covert Surveillance and Property Interference" and Covert Human Intelligence Sources". The Council takes responsibility for ensuring the RIPA procedures are continuously improved.

2. The authoritative position on RIPA is, of course, the Act itself and the associated Home Office Codes of Practice and any officer who is unsure about any aspect of this Document should contact, at the earliest possible opportunity, the Senior Responsible Officer, namely the Head of Legal Services ("SRO") for advice and assistance. Appropriate training and development will be organised by the SRO

3. The Codes of Practice are admissible as evidence in Court. The provisions of the codes, if relevant, must be taken into account by the Court.

4. Copies of this Document and related Forms will be placed on the Intranet.

5. The SRO will maintain and check the Corporate Register of all RIPA authorisations. It is the responsibility of the relevant Authorising Officer, however, to ensure the SRO receives a copy of the relevant Forms as soon as possible.

6. RIPA and this Document are important for the effective and efficient operation of the Council's actions with regard to covert surveillance and Covert Human Intelligence Sources. This Document will, therefore, be kept under review by the SRO. Authorising Officers must bring any suggestions for continuous improvement of this Document to the attention of the SRO at the earliest possible opportunity.

7. If you are in any doubt on RIPA, this Document or the related legislative provisions, please consult the SRO at the earliest opportunity.

8. The Council treats its statutory responsibilities under t RIPA very seriously and expects Authorising Officers and applicants to do so also. Failing to adhere to this policy may result in disciplinary action being taken against Officers by the Council.

B. Background

The Human Rights Act 1998 requires the Council, and organisations working on its behalf, to have respect for the private and family life of citizens. However, in rare cases, it may be necessary for the Council to act covertly in ways that could interfere with an individual's rights.

The Regulation of Investigatory Powers Act 2000 (RIPA) provides a statutory mechanism for authorising directed surveillance and the use of a "covert human intelligence source" ("CHIS - e.g. an informer or undercover agent"). It aims to ensure that any interference with the individual's right to privacy under Article 8 of the European Convention is necessary and proportionate, and that both the public interest and the human rights of individuals are protected.

It also provides a mechanism for Council staff to access limited information from telecommunications companies which is covered in the Policy. All applications for the aquisition of communications data is dealt with through the National Anti –Fraud Network (NAFN), which acts as the Council's Single Point of Contact (SPOC).

It is important to note that the legislation does not just affect directly employed Council staff. All external agencies working for Caerphilly County Borough Council automatically become a public body under the Act for the time they are working for the council. It is essential therefore that all external agencies comply with RIPA too, and that work carried out by agencies on the Council's behalf be properly authorised by one of the Council's designated Authorising Officers.

The Office of The Surveillance Commissioners (OSC) can inspect the Council's policies and procedures and individual authorisations at any time. The OSC usually provide notice before an inspection, but can arrive unannounced. If the correct procedures are not followed the consequences can be serious. The evidence obtained may be ruled inadmissible. If officers are found to have acted in bad faith, a trial may be stopped as an abuse of process (R v Sutherland 2002 - police officers were found to have acted in bad faith in covertly recording conversations in the exercise yard between defendants and their solicitors). A complaint of maladministration might be made to the Ombudsman. The Council could be made the subject of an adverse report to the Surveillance Commissioner. A claim could be made leading to the payment of compensation by the Council. In any of these circumstances the Council is likely to receive adverse publicity.

This document summarises the relevant provisions of RIPA, the Codes of Practice and government guidance. If in doubt as to the application of these provisions officers are asked to refer to the relevant Home Office Codes of Practice (HHPS://www.gov.uk/government/organisations/home-office/series/ripa-codes) and to contact the Head of Legal Services if in any doubt as to how to apply the provisions.

C. Changes To The RIPA Process

The Protection of Freedoms Act 2012 came into force on 1st November, 2012 and requires all RIPA authorisations to obtain judicial approval by a court order before they can take effect.

The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 also came into force on 1st November, 2012 and limits the authorisation of directed surveillance to criminal offences which carry a custodial sentence of at least six months or relate to the sale of tobacco and alcohol to children ("the directed surveillance crime threshold").

D. What RIPA Does and Doesn't Do - Surveillance

RIPA does

- Require authorisation of directed surveillance
- Prohibit the council from carrying out intrusive surveillance
- Require authorisation of the conduct and use of CHIS
- Require safeguard for the conduct and use of a CHIS

RIPA does not

- Make unlawful conduct which is otherwise lawful
- Prejudice any existing power to obtain information by any means not involving conduct that may be authorised under the Act. For example, it does not affect the Council's current powers to obtain information via the DVLA or to obtain information from the Land Registry as to the owner of a Property.
- Apply to activities outside the scope of Part II of the RIPA, which may nevertheless be governed by other legislation, including the Human Rights Act. A public authority will only

engage RIPA when in performance of its 'core functions' - i.e. the functions specific to that authority as distinct from all public authorities.

Legal advice should always be sought if there is any doubt as to whether the activity in question is a 'core function'.

E. Types Of Surveillance

"Surveillance" includes:

- Monitoring, observing, listening to persons, their movements, conversations, other activities or communications;
- Recording anything monitored, observed or listened to in the course of surveillance; (this includes filming audio recording or writing down)
- Surveillance by, or with, the assistance of a surveillance device (this would include the use of binoculars)

Surveillance can by overt or covert

1. Overt Surveillance

Most of the surveillance carried out by the Council will be done overtly there will be nothing secretive, clandestine or hidden about it. In many cases, officers will be behaving in the same way as a normal member of the public (e.g. in the case of some test purchases), and/or will be going about council business openly. Similarly, surveillance will be overt if the subject has been told it will happen (e.g. where a noisemaker is warned that noise will be recorded if the noise continues, or where a premises licence for regulated entertainment is issued subject to conditions and the licensee is told that officers may visit without identifying themselves to check that the conditions are being met).

2. Covert Surveillance

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

RIPA regulates two types of covert surveillance - Directed Surveillance and Intrusive Surveillance - and the use of Covert Human Intelligence Sources (CHIS).

3. Directed Surveillance

Directed Surveillance is surveillance which

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

- Is undertaken for the purpose of a **specific investigation** or operation in a manner **likely to result in obtaining private information** about an individual (whether or not that person is specifically targeted for purpose of an investigation).

- Satisfies the directed surveillance crime threshold.

4. **Private Information**

Private information in relation to a person includes any information relating to his private or family life. 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 may very well result in the obtaining of private information. Similarly, although overt town centre CCTV cameras do not normally require authorisation, if the camera is tasked for a specific operation, which involved prolonged surveillance on particular individual/s, authorisation may well be required. The way in which a person runs her/his business may also reveal information about her or his private life. In deciding whether certain covert surveillance does, or does not, require a directed surveillance authorisation the potential applicant officer must carefully consider the issue of private information. There are, for example, test purchase situations and covert inspection activities where it is unlikely that any private information will be obtained and therefore no authorisation is necessary. However, in the event of subsequent legal proceedings, such a decision could be subject to challenge. It is therefore recommended that a decision not to seek authorisation be made in consultation with an authorising officer and that the decision making process be documented in accordance with the relevant department's internal procedures. For the avoidance of doubt, only those officers authorised to be 'Authorising Officers' for the purpose of RIPA can authorise directed surveillance **IF AND ONLY IF**, the RIPA authorisation procedures detailed in the Policy are followed.

5. **Directed Surveillance Crime Threshold (In Effect From 1 November, 2012)**

- The Council can only authorise use of directed surveillance under RIPA to prevent or detect criminal offences that are either punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment.

- The Council may also continue to authorise the use of directed surveillance for the purpose of preventing or detecting specified criminal offences under s146, 147 or 147A of the Licensing Act 2003 or Section 7(1) of the Children and Young Persons Act 1933 (relating to the underage sale of alcohol and tobacco) where the necessity and proportionality test is met and prior court approval has been granted.

Examples of cases where the offence being investigated attract a maximum custodial sentence of six months or more could include more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud. The Council may not authorise the use of directed surveillance under RIPA to investigate disorder that does not involve criminal offences or to investigate low-level offences which may include, for example, littering, dog control and fly-posting.

6. **Surveillance Must Be Necessary & Proportionate**

RIPA provides that before granting an authorisation the Authorising Officer must be satisfied that the proposed surveillance is necessary for the prevention or detection of crime or the preventing of disorder and is proportionate to what is sought to be achieved by carrying it out. Surveillance will not be proportionate, if the information sought could reasonably be obtained by less intrusive means. In particular, the Authorising Officer must consider both the gravity of the conduct under investigation and whether all reasonable alternative methods of obtaining the necessary outcome have been considered - and why they were discounted.

Council Officers can carry out "Directed Surveillance" IF AND ONLY IF the RIPA authorisation procedures are followed.

7. **Use of CCTV Cameras**

The use of temporary covert CCTV cameras at specified locations, e.g. fly tipping 'hotspots', for the purpose of recording unlawful activities and obtaining photographic evidence of the suspect/s, carries with it not only the potential to obtain personal data about the alleged offender/s but also the likelihood of collateral intrusion in to the activities of members of the public using the area under surveillance. In such circumstances authorisation will be required for directed surveillance.

Overt CCTV cameras which are permanently sited for the purposes of, for example, monitoring traffic flow or public safety will not generally require RIPA authorisation. Members of the public should be made aware that such systems are in use e.g. clearly visible cameras or signage, through the provision of information and by undertaking consultation. Guidance on their operation is provided in the Surveillance Camera Code of Practice issued under the Protection of freedoms act 2010.

However, there may be occasions, when the Council wishes to use such CCTV cameras for the purposes of a specific investigation or operation or to target a specific person. In such circumstances (unless as an immediate response to events) consideration must be given as to whether authorisation for directed surveillance is required. For example, authorisation for directed surveillance is likely to be required if the Council wishes to make use of permanently sited overt CCTV cameras in circumstances where officers have received reports of unlawful trading and wish to use those existing CCTV systems to keep watch for such activities. However, authorisation would not be required where officers review existing CCTV footage of general filing in the area for evidence of past unlawful activity following such a report.

8. **Collaborative Working**

If the Council is acting on behalf of another agency, or vice versa, the tasking agency should normally obtain or provide the RIPA authorisation. Where the operational support of another agency (e.g. the Police) is foreseen this should be specified in the authorisation.

For example, if the Police wish to use the Council's CCTV cameras for one of their investigations, this must be agreed by an Authorising Officer. A copy of the Police RIPA authorisation form must be obtained and a copy retained in the departmental records and a copy provided to Head of Legal Services for noting in the Central Register.

A Council officer seeking an authorisation should be alert to any particular sensitivities in the local community and if necessary consult with a senior Police Officer to ensure that the proposed surveillance creates no conflict with the activities of other public authorities.

Where an individual or non-governmental organisation is acting under the direction of the Council they are acting as an agency of the Council and any directed or intrusive surveillance they undertake must be considered for authorisation.

9. **Intrusive Surveillance**

- Is covert
- Relates to residential premises and private vehicles; and

- Involves the presence of an individual on the premises or in the vehicle; or is carried out by a surveillance device. If a surveillance device is not on the premises or in the vehicle it is not intrusive, unless it consistently provides information of the same quality as if it was on the premises or in the vehicle

- Also includes directed surveillance under the ambit of the Regulation of Investigatory Powers (Extension of Authorisation Provisions Legal Consultations) Order 2013

- Can be carried out only by Police and other specified law enforcement agencies.

Council officers must not carry out intrusive surveillance.

10. **Examples Of Different Types Of Surveillance**
Surveillance will fall into one of four categories:

Type of Surveillance	Examples
Overt	• Police Officer or Parks Warden on patrol. • Signposted town centre CCTV cameras (in normal use) • Recording noise coming from premises after the occupier has been warned that this will occur if the noise persists. • Some tests purchases (where the test purchaser behaves no differently from a normal member of the public).
Covert, but not requiring authorisation	• Hidden CCTV cameras providing general traffic crime or public safety information • General observations forming part of the legislative functions of officers as opposed to pre-planned surveillance of a specific person or group • Some test purchases (where the test purchaser behaves no differently from a normal member of the public.
Directed - requires RIPA authorisation	• Officers follow an individual over the course of the day, to establish whether he is working when claiming benefit. • Test purchases when the officer has a hidden camera or recording device to read information if this is likely to include information about the private life of a shop owner e.g. where he/she is suspected of running his business in an unlawful manner. • Covert cameras at a fly tipping hotspot.
Intrusive - the Council cannot do this	• Planting a listening device (bug) in a person's home or in their private

	motorcar.

Covert surveillance for any purpose other than the prevention or detection of crime should be conducted under other legislation, if relevant and RIPA authorisation should NOT be sought. This would include the surveillance for the ordinary functions carried out by all authorities such as employment issues, investigating long term sickness, contractual arrangements etc. The Council may only engage the use of RIPA when it is carrying out its "core functions" relating to enforcement. The disciplinary of an employee is not such a core function.

However, in exceptional circumstances, e.g. impact on public protection/safety, then it may be necessary to undertake covert directed surveillance other than by using RIPA. Under such circumstances, which should be rare, an application must be completed and the application must be clearly endorsed in red "NON RIPA SURVEILLANCE". The relevant application forms are set out in Part B of Appendix 3. The application must be submitted to a RIPA Authorising Officer in the usual way, who must consider it under the "necessity" and "proportionality" tests in the same fashion as they would a RIPA application. The normal procedures of timescales, reviews and cancellation must be followed:-

The SRO will keep a separate record of non- RIPA activities in the same manner as RIPA authorised activities.

Under no circumstances is this facility to be used to circumvent the usual procedures in relation to RIPA and Judicial Approval.

Directed and Intrusive Surveillance are subject to the Covert Surveillance & Property Interference Code of Practice (CoP) issued under s 71 RIPA.

F. Conduct & Use Of A Covert Human Intelligence Source (CHIS)

1. Who Is A CHIS?

- A person is a CHIS if s/he establishes or maintains a personal or other relationship with a person for the covert purpose of obtaining information, or access to information, or covertly discloses information obtained by the use of such a relationship.

- A covert purpose is one calculated to ensure that one of the parties to the relationship is unaware of the purposes.

- The Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013 further defines a "relevant source" as a CHIS who holds a position or office within a police force or the Home Office and enhanced authorisation arrangements are in place for this type of source (previously known as "undercover officers").

2. What Must Be Authorised

The conduct or use of a CHIS requires <u>authorisation</u>

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

- **Use** of a CHIS = actions inducing, asking or assisting a person to act as a CHIS.

The Council can use a CHIS IF AND ONLY IF RIPA procedures are followed.

3. **European Convention On Human Rights (ECHR)**

Authorisations for the use or conduct of a CHIS relate to the covert manipulation of a relationship to gain any information. ECHR case law makes it clear that Article 8 includes the right to establish and develop relationships. Accordingly, any manipulation of a relationship by a public authority is likely to engage Article 8, regardless of whether or not the public authority intends to acquire private information. The Council should consider an authorisation whenever the use or conduct of a CHIS is likely to engage an individual's rights under article 8, whether this is through obtaining information, particularly private information, or simply through the covert manipulation of a relationship. An authorisation will be required if a relationship exists between the subject and the CHIS, even if specific information has not been sought by the public authority.

Legend Building - when a relevant source is deployed to establish their 'legend/build up their cover profile, an authorisation must be sought under the 2000 Act if the activity will interfere with an individual's Article 8 rights. The individual does not have to be the subject of a future investigation. Interference with any individual's Article 8 rights requires authorisation under the 2000 Act.

4. **Juvenile Source**

Special safeguards apply to the use or conduct of juvenile sources (under 18). Only the Chief Executive can authorise the use of a juvenile source. Under no circumstances can a child under 16 years of age be authorised to give information against his or her parents.

5. **Vulnerable Individuals**

A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself or herself, or unable to protect himself or herself against significant harm or exploitation. A vulnerable individual should only be authorised to act as a source in the most exceptional circumstances. Only the Chief Executive can authorise the use of a vulnerable person as a CHIS

6. **Test Purchases**

If a source is to be asked to obtain information, provide access to information or otherwise to act for the benefit of the Council, then a CHIS authorisation for the use or conduct of that source will be required in advance of any such assignment which requires the source to establish or maintain a 'person or other relationship' for a covert purpose. In this context 'establish' simply means 'set up' (as distinct from 'maintain'), so that even a single transaction -e.g. in the case of a test purchase - may constitute a relationship. Repetition is not always necessary to give rise to a relationship, but whether or not a relationships exists depends on all the circumstances including the length of time of the contract between the seller and buyer and the nature of any covert activity. Some assignments are unlikely to require the source to establish a personal or other relationship for a covert purpose - e.g. if the source's assignment is limited to gathering factual information about the layout of commercial premises.

If a Council officer, or another person acting under the instructions of a Council officer, enters a shop in the normal course of business and purchases a product available for sale over the counter then a CHIS authorisation will not normally be required. However, unless the test purchaser is to be instructed not to enter in to any conversation with the shopkeeper then consideration must be given as to whether there is the possibility of a 'relationship' which would require a CHIS authorisation.

If an officer develops a relationship with a shopkeeper in order to obtain information about the source of the allegedly illegal products on sale, then the officer will require a CHIS authorisation.

If a Council officer, or another person acting under the instructions of an officer, uses any covert recording device (camera and/or audio) to record events in the shop then an authorisation will be required for directed surveillance.

7. **Members Of The Public**

The provisions of RIPA are not intended to apply in circumstances where members of the public volunteer information to the Council as part of their normal civic duties, or to contact numbers set up to receive information. Members of the public who volunteer information to the Council, whether anonymously - e.g. by means of a telephone line set up for that purpose or otherwise, will not normally be considered to be a CHIS. However, if a member of the public is asked to e.g. watch out for and diarise particular activities at specific times about another person with whom they have a relationship (whether personal or not) then this would amount to directed surveillance and a CHIS authorisation would be required.

8. Noise

Persons who complain about excessive noise, and are asked to keep a noise diary, will not normally be a CHIS, as they are not required to establish or maintain a relationship for a court purpose. Recording the level of noise *(e.g. the decibel level) will not normally capture private information and therefore does not require authorisation. Recording sound with a DAT recorder on private premises could constitute intrusive surveillance unless it is done overtly - for example it will be possible to record sound if the noisemaker is warned that this will occur if the level of noise continues.

G. Online Covert Activity

The use of the internet may be required to gather information prior to and/or during an operation, which may amount to directed surveillance. Alternatively an investigator may need to communicate covertly online, for example, contacting individuals using social media websites.

Whenever the Council intends to use the internet as part of an investigation, we must first consider whether the proposed activity is likely to interfere with a person's Article 8 rights, including the effect of any collateral intrusion. Any activity likely to interfere with an individual's Article 8 should only be used when necessary and proportionate to meet the objectives of a specific case.

Where it is considered that private information is likely to be obtained, an authorisation (combined or separate) must be sought. Where an investigator may need to communicate covertly only, a CHIS authorisation should be considered.

The use of disguised purchaser details in a single, overt, electronic purchase does not require a CHIS authorisation because no relationship is usually established at this stage.

Use of social media for the gathering of evidence to assist in enforcement activities must also comply with the policy set out below:

Social Media & Online Covert Activity Policy

- It is not unlawful for a Council officer to set up a false identity, but it is inadvisable to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

- Where it is necessary and proportionate for officers pursuing an investigation to create a false identity in order to 'friend' individuals on social networks a CHIS authorisation must be

obtained. If such activity is likely to result in the obtaining of private information, a Directed Surveillance authorisation (combined with a CHIS authorisation or separate) must be obtained.

- Authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a Council officer (i.e. the activity is more than mere reading of the site's content). Where activity is only carrying out a test picture a CHIS authorisation may not be necessary, but this should be confirmed with the Authorising Officer on a case by case basis.

- Where privacy settings are available, but not applied, the data may be considered open source and an authorisation is not usually required.

- Officers viewing an individual's open profile on a social network should do so as infrequently as possible in order to substantiate or refute an allegation.

- Where repeated viewing of open profiles on social networks is necessary and proportionate to gather further evidence or to monitor an individual's status, then RIPA authorisations must be considered as repeat viewing of "open source" sites may constitute directed surveillance on a case by case basis. Any decision not to seek authorisation be made in consultation with an authorising officer and that the decision making process be documented in accordance with the relevant department's internal procedures.

- Officers should be aware that it may not be possible to verify the accuracy of information on social networks and, if such information is to be used as evidence, take reasonable steps to ensure its validity.

H. Surveillance Devices & Other Technical Equipment

A CHIS who is authorised to wear or carry a surveillance device, such as a recording device, does not require a separate directed surveillance authorisation, provided the device will only be used in the presence of the CHIS, even if this takes place inside a residential premise or private vehicle.

Each Division should maintain a register of all equipment that is used for surveillance work. This equipment could include surveillance vehicles, cameras, video recorders and binoculars. Specific individuals should be given responsibility for issuing the equipment from the storage location. Every time each item of equipment is issued for surveillance purposes a record should be made of the following:

- Identification of equipment
- RIPA authorisation number for which the equipment is being used
- Date the equipment was issued
- Person taking possession of the equipment
- Date the equipment was returned to the Divisional Store

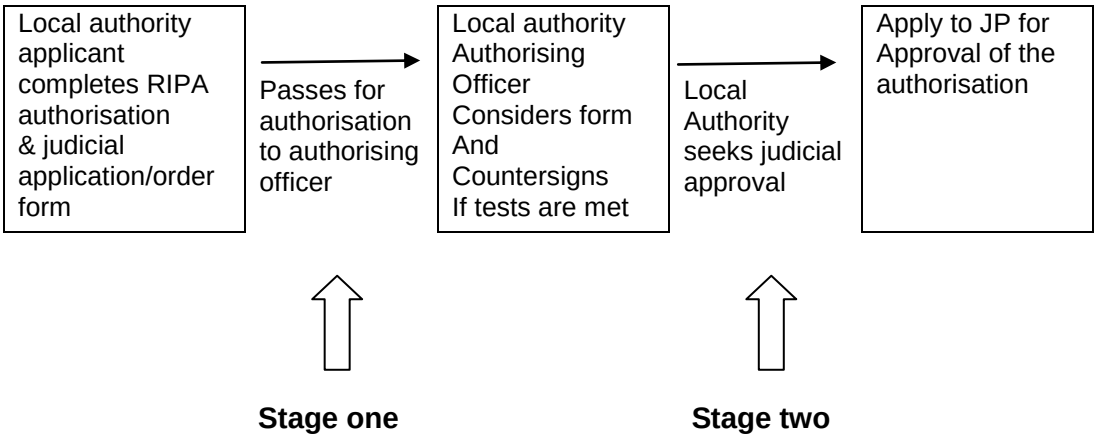
If equipment is issued to a particular officer on a long term basis where it might also be used for purposes other than covert surveillance, the officer should record on the equipment register any occasions when that equipment is being used for covert surveillance. For instance this could apply to the issuing of binoculars or a camera. However if equipment such as a camera is issued to an officer, but it is only used to record evidence and not for any covert purpose then there is no requirement for such equipment to be recorded on the register.

I. Applications For Authorisation & Approval

Directed Surveillance and the use of a CHIS can only be carried out if the proper two stage RIPA authorisation and approval process is followed:

- Stage one - internal authorisation
- Stage two - approval by a magistrate

DIRECTED SURVEILLANCE/CHIS (COVERT HUMAN INTELLIGENCE SOURCE)



Appendix 1 provides a flow chart of process from application consideration to record of information.

Stage One - Internal Authorisation

1. **Application Forms**

Applications for authorisation should be made in writing using standard RIPA forms. The forms are designed to ensure that the criteria for RIPA are fully considered.

The forms are included in Appendix 3.

The Application Form must now be accompanied by the partly completed Magistrates Court Application Form.

2. **Grounds For Authorisation**

Directed Surveillance, or the Conduct and Use of a CHIS can be authorised by the Council only

- **For the prevention or detection of crime or the prevention of disorder which constitutes one or more criminal offence**

- AND

- At least one of the criminal offences is punishable, whether on summary conviction or on indictment, by a maximum term of imprisonment of at least six months of imprisonment

OR

- Is an offence under Section 146, 147 or 147A of the Licensing Act 2003 or Section 7 of the Children and Young Persons Act 1933;

The Conduct and use of the Covert Human Intelligence Sources (CHIS Forms) can be authorised by the County Borough Council only on the following ground:-

- For the purpose of preventing or detecting crime or of preventing disorder

3. Necessary, Proportionate, Collateral Intrusion & Confidential Material

4. What Does The Term "Necessary" Mean?

RIPA provides a framework for ensuring that any surveillance activities do not infringe the human rights of the individual. In considering whether to grant an authorisation, the authorising officer must consider whether the proposed conduct is necessary.

An Authorising Officer must consider a number of issues in deciding if a proposed course of action is necessary. These include:

- Balancing the "target's" human rights with the rights and freedoms of other individuals

- Deciding that the required information needs to be acquired in this way and that it cannot reasonably be acquired by other means that would involve less, or no, invasion of privacy.

Every case must be considered on its merits, as what is necessary in some circumstances is not necessary in others. Always consider other ways in which the information could be obtained, such as use of third party information powers, the Internet and other sources. The information must be necessary in order to carry out the investigation. The Council should not consider obtaining information through covert means that it does not need for the investigation. It might be nice to know and very interesting, but it is not strictly necessary to have it then, officers should not seek to obtain it. Officers need to show why it is necessary in this case and at this time.

5. What Does The Term "Proportionate" Mean?

Proportionality is a very important concept, and it means that any interference with a person's rights must be proportionate to the intended objective. This means that the action is aimed at pursuing a legitimate aim (for example, protecting a child from potential abuse). Interference will not be justified if the means used to achieve the aim are excessive in all the circumstances. Thus where surveillance is proposed that action must be designed to do no more than meet the objective in question, it must not be unfair or arbitrary, and the impact on the individual or group of people concerned must not be too severe.

Each action authorised should bring an expected benefit to the investigation and should not be disproportionate. The fact that a suspected offence may be serious will not on its own render intrusive actions proportionate. No action will be considered proportionate if the information sought could reasonably be obtained by other less intrusive means.

6. What Questions Should The Applicant Address On The Proportionality Part Of The Application Form?

The Applicant should address the following elements of proportionality:

(a) Balance the size and scope of the proposed activity against the gravity and extent of the perceived offence;

(b) Consider whether the activity is an appropriate use of RIPA and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result.

(c) Explain how and why the methods to be adopted will cause the least possible intrusion on the target and others;

(d) Evidence as far as reasonably practicable, what other methods had been considered and why they were not implemented.

7. What Does The Term "Collateral Intrusion" Mean?

Collateral intrusion occurs when officers obtain private landlord information about people unconnected with the investigation. Authorising Officers must consider the likelihood and extent of collateral intrusion when considering any application and ensure that Applicants have planned to minimise collateral intrusion. Where the collateral intrusion is unavoidable the activity may still be authorised, provided that the collateral intrusion is considered to be proportionate. Situations where collateral intrusion can occur include where:

- Observing how busy a business is, results in watching unconnected people come and go
- At a test purchase, we might observe or overhear other customers conversations

8. What Does The Term "Confidential Material" Mean?

Confidential material is anything

- That is subject to legal privilege, for example communications between a legal adviser and his/her client;
- That is a communication between a Member of Parliament Assembly Member/Member of European parliament and a constituent regarding constituency matters;
- That is confidential personal information, for example information about a person's health or spiritual counselling or other assistance given or to be given to him or her;
- That is confidential journalistic material (this includes related communications), that is material obtained or acquired for the purposes of journalism and subject to an undertaking to hold it in confidence.

  In cases where it is likely that knowledge of confidential material will be acquired, then the directed surveillance must be authorised by the Chief Executive.

9. Guidance For Applicants - Directed Surveillance

The information provided on the application form should:

- Identify the nature of the surveillance and the means by which it is to be undertaken;
- Specify when the surveillance is to start and the length of time it is expected to continue;

- Explain why the applicant believes that the proposed surveillance is necessary for the prevention or detection of crime or the prevention of disorder (as appropriate);
- Identify what is sought to be achieved by the proposed surveillance;
- Identify the offence which satisfies the directed surveillance crime threshold;
- Explain why the applicant considers the proposed surveillance is proportionate, having regard to the gravity and extent of the activity under investigation;
- Explain why the proposed surveillance is a reasonable method of obtaining the necessary outcome;
- Identify whether other reasonable means of obtaining information have been considered and why they have been discounted;
- Explain how and why the proposed surveillance will cause the least possible intrusion on the intended subject/s:
- Include an assessment of the risk of any collateral intrusion and details of any measures taken to limit this;
- Avoid any repetition of information.

10. Guidance For Applicants - Conduct & Use Of A CHIS

The information provided on the application form should:

- Identify the purpose for which the CHIS will be tasked or deployed (e.g. counterfeit sales);
- Identify the nature of the conduct and use of the CHIS and the period of time it is expected to continue;
- Explain why the applicant believes that the proposed conduct and use is necessary for the prevention or detection of crime or the prevention of disorder (as appropriate);
- Explain how each activity to be authorised is expected to bring a benefit to the investigation;
- Explain how and why the proposed conduct and use is proportionate to the intelligence dividend it hopes to achieve, having regard to the gravity and extent of the activity under investigation;
- Explain how and why the methods to be adopted will cause the least possible intrusion to the subject/s;
- Include an assessment of the risk of any collateral intrusion and details of any measures taken to limit this;
- Identify whether other reasonable methods of obtaining information have been considered and why they have been discounted;

- Ensure the confidentiality of the CHIS - i.e. not include information which could lead to the identification of the CHIS;

- Avoid any repetition of information.

Surveillance will not be proportionate if the information which is sought could reasonably be obtained by other less intrusive means

11. **Guidance For Authorising Officers**

Authorisations can only be granted by the Authorising Officers listed in **Appendix 2**.

Authorisations under RIPA is quite separate from delegated authority to act under the Council's scheme of delegation and internal departmental schemes of management. RIPA authorisations are for specific investigations only, and must be cancelled or renewed once the specific surveillance is complete or about to expire.

The Authorising Officer should not just "sign off" an authorisation, but must give **personal consideration** to the necessity and proportionality of the proposed action and must personally ensure that the surveillance is reviewed and cancelled within the applicable timescales.

The Authorising Officer should not “sign off” any operation that he/she has a direct involvement in.

In addition the Authorising Officer must also pay particular attention to Health and Safety Issues that may be raised as a result of any proposed surveillance activity. Under no circumstances should an Authorising Officer approve any RIPA form unless he/she is satisfied that the health and safety of Council employees/agents are suitably addressed and/or risks minimised so far as possible and proportionate with the surveillance being proposed

12. Assessing The Application Form

When considering whether to authorise surveillance an Authorising Officer must:

- Consider the relevant Code/s of Practice;

- Satisfy him/herself that the authorisation is **necessary** in the circumstances of the particular case to prevent or detect crimes and that the specified offence satisfies the directed surveillance crime threshold;

- Satisfy him/herself that the surveillance is **proportionate** to what it seeks to achieve. In assessing whether or not the proposed surveillance is proportionate, the Authorising Officer will consider other appropriate means of gathering information;

  If there is an alternative practicable means of carrying out the surveillance, which is less intrusive, then the surveillance is neither necessary nor proportionate and should not be authorised

- Take into account the risk of intrusion into the privacy of persons other than the specified subject of the surveillance (**Collateral Intrusion**). Measures must be taken wherever practicable to avoid collateral intrusion;

- Set a date for review of the authorisation, this should not exceed one month from the date of the grant of the authorisation;

- Record the expiry date of the authorisation on the application form. This will be three months (Directed Surveillance) or twelve months (CHIS) less one day from the date of the grant of the authorisation;

- Submit draft application for review by Gatekeeper and Obtain a Universal Reference Number (URN) for the application, from the SRO

- Ensure that the original form is completed and forwarded to the Council's Head of Legal Services who maintains the Council's central log, return one week of completion.

13. **Additional Factors When Authorising A CHIS**

In addition, when authorising the conduct or use of a CHIS the Authorising Officer must:

- Be satisfied that the **conduct** and/or **use** of the CHIS is proportionate to what is sought to be achieved;

- Be satisfied that appropriate arrangements are in place for the **management and oversight** of the CHIS, in particular the appointment of a named 'handler' to direct and record the day to day activities of the CHIS and monitor the CHIS's security and welfare, and the appointment of a named 'controller' to be responsible for the management of the handler and general oversight of the use of the CHIS;

- Consider the likely degree of intrusion of all those potentially affected;

- Ensure that a risk assessment is carried out to determine the risk to the CHIS of the activities to be undertaken and the likely consequences should the CHIS's role become known;

- Consider any adverse impact on community confidence that may result from the use or conduct or the information obtained; and

- Ensure **records** contain statutory particulars and are not available except on a 'need to know' basis.

14. **Duration Of Authorisations**

- The authorisation **must be cancelled** once it is no longer needed, and otherwise lasts for a maximum of 3 months for Directed Surveillance and 12 months for a CHIS (one month for a juvenile).

15. **Review & Cancellation**

Review: The Authorising Officer must review authorisations at regular recorded intervals (normally not more than one month) and must cancel an authorisation if s/he becomes satisfied that the surveillance or use of a CHIS is no longer required or appropriate. The review of the use of a CHIS should include the use made of the CHIS during the period authorised, the tasks given to the CHIS, the information obtained from the CHIS, and the reasons why executive actions is not possible at this stage. The results of a review should be retained for at least three years. Frequent reviews should occur when the use of a CHIS provides access to confidential information or involves significant collateral intrusion.

The authorising officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable, but should not prevent reviews being conducted in response to changing circumstances.

Cancellation: The authorising officer who granted or renewed the authorisation must cancel it if they are satisfied that the use of the surveillance or the use or conduct of the CHIS no longer satisfied the criteria for authorisation or that arrangements for the CHIS's case no longer satisfy the requirements described in section 29 of the 2000 Act. Where necessary, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled. The Authorising Officer will wish to satisfy themselves that all welfare matters are addressed. When cancelling the authorisation, the Authorising Officer should record whether the surveillance was effective, necessary and met its objectives. Cancellations must be made using the cancellation form. If during an investigation it becomes clear that the activity being investigated does not amount to an offence which would meet the directed surveillance crime threshold, the Applicant must submit an application to an Authorising Officer for the authorisation to be cancelled. Cancellations do not need to be submitted for court approval.

If it becomes necessary to amend the terms of an authorisation to reflect information gathered in the course of surveillance then a review should be conducted for that purpose. For example, if a directed surveillance authorisation provides for the surveillance of unidentified individuals whose identity is later established, the terms of the authorisation should be refined at a specially convened review to include the identity of these individuals.

16. **Renewals**

Authorisations can be renewed in writing prior to expiry of the maximum period. The Authorising Officer must consider the matter afresh by carrying out a further review, including taking into account the information obtained and benefits of the surveillance to date, why it is considered necessary for the authorisation to continue and any collateral intrusion that has occurred.

The renewal will begin on the day when the authorisation would have expired. Authorisation may be renewed more than once if still considered necessary and proportionate. **All renewals must also now be approved by the court.**

17. **Forms**

All RIPA forms (applications, review, renewal and cancellation), must be forwarded to the SRO within one week of the relevant authorisation, review, renewal, cancellation or rejection).

18. **Urgent Authorisations**

Urgent oral authorisations can no longer be granted. ALL authorisations must be in writing and submitted to the court with the completed court form. In exceptional circumstances an out of hours court application may be made, but a signed written authorisation will still need to be produced to the court (see below).

Stage 2 Magistrates Approval

Magistrates Approval

19. After the Authorising Officer has signed the RIPA application form, it must be approved by a Magistrate before the operation can commence. The investigating officer should liaise as necessary with Legal to seek this authorisation, if they require advice or assistance in relation to the process .

Application & Attendance

.20. **A hearing with the Court to seek Judicial Approval shall be arranged The Court should be provided with** the RIPA application form *(signed by the Authorising Officer) and supporting information. **A duly Authorised officer, normally the applicant** will be required to attend court to seek the Magistrate's approval.with assistance from Legal if required.

Guidance on the procedure for seeking Magistrate's approval can be found at : https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa.

J. **Acquisition Of Communications Data**

1. **What Is Communication Data?**

Communication data means any traffic or any information that is or has been sent over a telecommunications system or postal system, together with information about the use of the system made by any person.

2. RIPA defines communications data in three broad categories:-

(a) **Section 21(4)(c) Information About Communications Service Users**
This category mainly includes personal records supplied to the Communications Service Provider (CSP) by the customer/subscriber. For example, their names and address, payment method, contact number etc.

(b) **Section 21(4)(b) Information About The Use Of Communications Services**
This category mainly includes everyday data collected related to the customer's use of their communications system. For example details of the dates and times they have made calls and which telephone numbers they have called.

(c) **Section 21(4)(a) Information about Communications Data (Traffic Data)**
This category mainly includes network data generated by the CSP relating to a customer's use of their communications system that the customer may not be aware of. For example, cell site data and routing information.

3. **The Council only has power to request data under Section 21(4)b and Section 21(4)c but NOT Section 21(4)(a)**

4. **<u>What Types Of Communications Data is Available To The Council?</u>**

Section 21(4)(c) – Information About Communications Service Users

- Name of account holder/subscriber
- Installation and billing address
- Method of payment/billing arrangements
- Collection/delivery arrangements for a PO Box (i.e whether it is collected or delivered – not where it is collected from or delivered to)
- Other customer information such as any account notes, demographic information or sign up data (not passwords or personalised access information).

4. **Section 21(4)(b) – Information About The Use Of Communication Services**

- Outgoing calls on a landline telephone or contract or prepay mobile phone
- Timing and duration of service usage
- Itemised connection records
- E-mail logs (sent)
- Information about the connection, disconnection and re-connection of services
- Information about the provision of conference calling, call messaging, call waiting and call barring
- Information about the provision and use of forwarding/redirection services (postal and telecom)
- Records of postal items, such as records of registered, recorded or special delivery postal items, records of parcel consignment, delivery and collection.

6. **What Purpose Can Communications Data Be Accessed**

The Council's can only access communications data for the **prevention and detection of crime or preventing disorder** (Section 22(2)(b) of RIPA).

7. Applying For Communications Data

The investigating officer must complete an application form (https://www.gov.uk/government/organisations/home-office/series/ripa-forms-2) in full with no sections omitted. (The form is subject to inspection by the Interception of Communications Commissioner and the applicant may be asked to justify their application).

Two forms of authorisation are possible:-

(a) An authorisation under Section 22(3) of RIPA. This authorises the applicant to personally extract the data from the CSP's records. (This will rarely be used by the Council as its intended use is where there may be a security breach at the CSP and asking the CSP to provide the data would forewarn or alert the subject).

(b) A notice under Section 22(4) of RIPA requiring the CSP to extract the communications data specified from its records and to send that data to the Single Point of Contact (SPOC) (normal request).

The applicant must indicate which authorisation they seek.

The application form is then submitted to the SPOC for the Council, which is the National Anti-Fraud Network (NAFN).

The idea of only having one point of contact for each public authority was agreed between the Home Office and the CSP's to ensure data was only supplied to those entitled to obtain the data. Only SPOC can acquire communications data on behalf of the Council.

The SPOC will then assess whether the form is completed properly, that the request is lawful, the request is one to which the CSP can practically respond and that the cost and resource implications for the CSP/Council are within reason.

The SPOC will then submit the form to the Authorising Officer for authorisation. (As previously stated, the application form is subject to inspection by the Interception of Communications Commissioner and therefore the Authorising Officer may be called upon to justify any decisions made).

The application must then be approved by a Magistrate. The Investigating Officer /duly authorised officer should if required liaise with Legal to obtain this authorisation.

The Investigating Officer /duly authorised officer with assistance from the legal team (if necessary) will arrange a hearing with the Court to seek the Magistrate's approval. They should provide the Court with the application form and supporting information. **A duly Authorised officer, normally the applicant /**Investigating Officerwill be required to attend Court to seek the Magistrate's approval.

Guidance on the procedure for seeking Magistrates' approval can be found at https://www.gov.uk/government/publications/changes-to-local-authority-use of ripa

If the application is rejected by either the SPOC or the Magistrates, the SPOC will retain the form and inform the applicant in writing of the reasons for its rejection.

Once authorised by the Magistrates, the SPOC will forward the application to the CSP.

Once the data sought is returned to the SPOC, a copy of the information will be passed to the applicant.

All original documents will be retained by the Investigating Officer.

There are a number of other administrative forms that the SPOC's are obliged to complete as the application is progressed, although these will not necessarily involve the Investigating Officer.

Authorisations to collect communications data under S22(3) have a life span of one month. However, they can be renewed by serving a new authorisation or notice for further months ,within any time within the current life of the notice. Magistrates would need to approve any renewal..

If you are at all unsure about anything to do with acquiring communication data, please contact either the SPOC, the Head of Legal Services or the Deputy Monitoring Officer for advice **before** applying.

The Head of Legal Services is the Senior Responsible Officer for the Council.

K. Record Maintenance

The Council must keep a secure centrally retrievable record of all authorisations, reviews, renewals and cancellations.

1.. Universal Reference Number For Authorisations

The Head of Legal Services will allocate a Universal Reference Number (URN) to each application, this will be assigned by the Gatekeeper, the Corporate Solicitor, once satisfied that the application is acceptable.

2. Records Maintained in the Service Area

The following documents must be retained in the department:

- A copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the authorisation given by the Authorising Officer.
- A copy of the court application and order;
- A record of the period over which the surveillance has taken place;
- The frequency of review prescribed by the Authorising Officer;
- A record of the result of each review of the authorisation;
- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- A copy of the court application and order for any renewal;
- The date and time when any instruction was given by the Authorising Officer;
- The Universal Reference Number for the authorisation (URN).

The same principles or record keeping apply to applications which are refused.

A separate record should be maintained for human sources who do not meet the definition of a CHIS - e.g. members of the public who volunteer information on a repeated basis - as this will assist Officers in determining if and when that should may become a CHIS.

Copies of authorisations, reviews, renewals and cancellations may be disclosed in legal proceedings. If proper records are not maintained, evidence gathered may be inadmissible.

3. Central Records

The Council's SRO must maintain a Central Record, Authorising Officers must forward the original authorising form (and any review/renewal/cancellation and rejection of the same) plus a copy of any judicial approval order from as soon as is practicable. The SRO will monitor the same and give appropriate guidance, from time to time, or amend this Document as necessary.

The Central Record for directed surveillance will consist of

- Date of authorisation
- Name & grade of Authorising Officer
- A unique Reference Number for the investigation
- Title of operation including the names of the subjects if known
- Whether urgency provisions used
- Details of attendances at the Magistrates' Court for judicial approval. (This will consist of the date of attendance at Court, the determining Magistrate, the decision of the Court and the time and date of that decision)
- Dates of any reviews
- Date of renewal

- Name and grade of Authorising Officer granting renewal
- Whether investigation is likely to result in obtaining confidential material
- Date of cancellation

All forms must be sent to the SRO in sealed envelopes and marked “strictly private and confidential”.

The Council will retain records for a period of at least three years from the ending of the authorisation. The Office of the Surveillance Commissioners (OSC) can audit/ review the Council’s policies and procedures and individual authorisations.

4. **Gatekeeper Role**

As a number of different Authorising Officers are entitled to authorise the use of directed surveillance or the use of a CHIS it is important that the quality of all such authorisations is checked for consistency by or on behalf of the SRO.

The Council’s Corporate Solicitor will undertake a gate keeper role and detail all the authorisations when they are received at the central register,on behalf of the SRO. If any such authorisation is found not to meet the high standards expected in the Authority the Gatekeeper on behalf of the SRO will instruct the Authorising Officer to immediately cancel the authorisation. If the difficulties can be overcome, a new application must be made by the Applicant and carefully assessed by the Authorising Officer, bearing in mind the concerns expressed by the Gatekeeper.If it is decided that the granting of an authorisation for this investigation will not be appropriate, for reasons of lack of necessity or proportionality or otherwise, the Applicant will be instructed that no surveillance may be used in this investigation.

5. **Records Maintained Centrally By SRO**

11. Authorising Officers must forward the original of each authorisation, review, renewal, cancellation form, court application form and court order to the Head of Legal Services. All forms must be sent in sealed envelopes and marked ‘Strictly Private and Confidential’.

L. Oversight Review & Amendments

1. Oversight Procedures

The SRO shall establish and maintain regular meetings not less than twice a year with the Gatekeeper and Authorising Officers to check and test processes and address any training requirements. The SRO shall arrange an oversight meeting as soon as practicable following an inspection to discuss issues and outcomes as appropriate.

The SRO shall record any issues arising out of authorisation applications, the statutory considerations, reviews and cancellations and shall review the quality of authorisations granted from time to time.

The SRO shall carry out analysis of such issues and shall decide appropriate feedback to the Authorising Officers.

2. Reviews

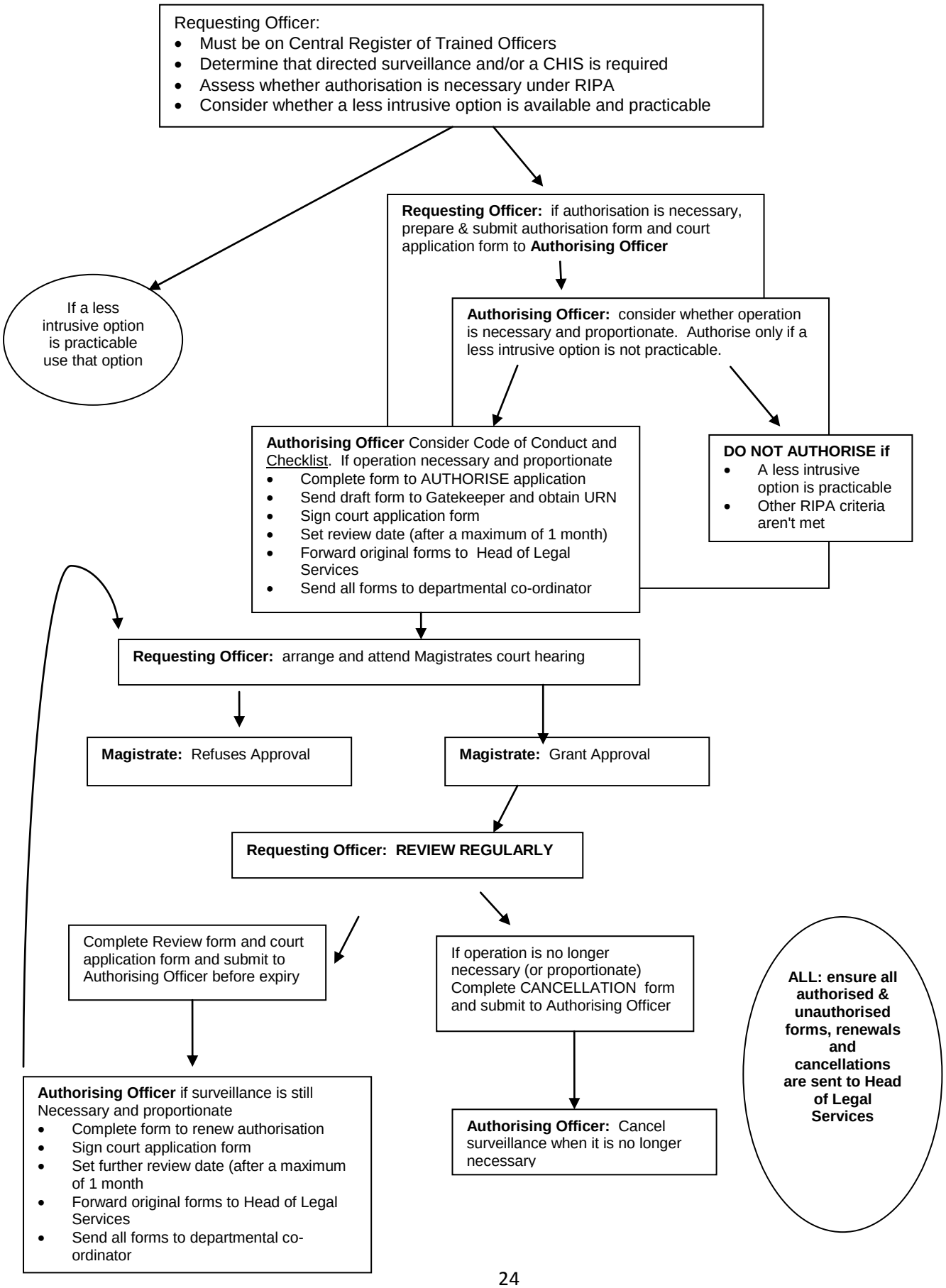
The number of RIPA operations undertaken by the Council shall be reported quarterly to the Council's Audit Committee. In addition in relation to Public Protection Operations, the number and type of RIPA and Communications Data Requests and their results are also reported annually to the relevant scrutiny committee.

This Policy will be reviewed every two years and will be reported to Cabinet for approval.

3. Amendments To This Policy & Procedure

The SRO is duly authorised to keep this guidance document up to date, and to amend, delete, add or substitute any provisions as s/he deems necessary. For administrative and operational effectiveness, s/he is also authorised to amend the list of Authorising Officers set out in Appendix 2, by adding, deleting or substituting any posts.

Appendix 1 - Flow Chart Of Process



Appendix 2 Authorising Officers

Authorising Officers must be a Director, Head of Service, Service Manager or equivalent. The Authorising Officer should not be directly involved in the investigation. Authorising Officers are listed below:

The Chief Executive

ONLY the chief Executive, (or in her absence the person acting as CEO) can authorise:

- The use of a juvenile (i.e. under 18) or a Vulnerable Person to be a CHIS;

- Operations where confidential information may be obtained. Confidential information includes confidential personal information, confidential constituent information, confidential journalistic material and communications subject to legal privilege. Confidential personal information includes information held in confidence relating to the physical or mental health or spiritual counselling of a person who can be identified from it.

Legal advice should always be sought in these circumstances

Other Authorising Officer

The Council's Authorising Officers can authorise applications from any department but should be independent of the investigation in respect of which authorisation is sought.

With effect from 1st September, 2015 the Authorising Officers are:

Head of Legal Services
Head of Public Protection
Trading Standards, Licensing and Registrars Manager
Deputy Monitoring Officer

Senior Responsible Officer

The SRO is responsible for ensuring the integrity of the Council's processes for authorising directed surveillance and the use of CHIS's and ensuring compliance with RIPA and is the principal point of contact with the Office of Surveillance Commissioners and Inspectors when they conduct their inspections. The Council's Senior Responsible Officer is the Council's Head of Legal Services.

Authorising Officer/Designated Person for Acquisition of Communication Data with effect from 1st September 2015 are :

- Head of Public Protection
- Deputy Monitoring Officer

Appendix 3 Forms

Part A

Authorisation - Directed Surveillance

- Application
- Cancellation
- Review
- Renewal

Authorisation - CHIS

- Application
- Cancellation
- Review
- Renewal

Court Approval/Application Order

Part B

Human Rights Act 1998 – Additional Forms

- Authorisation for approval to carry out activity potentially in interference with Qualified Human Rights.