DENBIGHSHIRE COUNTY COUNCIL

Corporate Policy & Procedures
For Denbighshire County Council Employees on the Regulation of Investigatory Powers Act 2000

CET/R23
Version 10 (2021)

THE REGULATION OF INVESTIGATORY POWERS ACT 2000

CONTENTS PAGE

FOREWORD

This Corporate Policy and Procedures has been produced for the use of Denbighshire County Council Employees and any relevant contractors employed by the Council. All relevant Council contracts will includes a term that this policy is to be observed by any Contractor acting on behalf of the Council. Its provisions must be followed, where they apply, by all Officers. In addition, all employees must use only the Authorising Forms that are available on the Home Office website for authorisation purposes.

This policy has been developed in consultation with representatives from across the departments performing surveillance. This policy replaces any previous policy and procedures. A copy of this policy together with the Home Office Codes of Practice and the Investigatory Powers Tribunal leaflets will be made available for public inspection at Council offices. The policy is also available on the Council's website.

In addition a copy of this document will be readily available to all employees, and a copy may be found on the Denbighshire Information Centre. This Policy has been produced in English and Welsh, and any comments or observations on its contents may be made to the Head of Legal and Democratic Services /Monitoring Officer who also acts as the Council's Senior Responsible Officer in respect of RIPA.

If you are unclear as regards any aspect of this document, you should contact the Head of Legal, HR and Democratic Services.

Any minor amendments to this policy will require the approval of the RIPA Working Group. Any substantial amendments to policy will require additional approval of the Council's Corporate Governance Committee and Cabinet.

January 2021

CHAPTER 1: INTRODUCTION

1.1 The Human Rights Act 1998 became part of UK law on the 2nd October 2000, making it unlawful for a "public authority"' (which includes a Local Authority) to breach any Article of the European Convention on Human Rights. The Act also made provision for any person who has suffered as a result of a breach of the European Convention on Human Rights to seek redress within the UK domestic courts, without having to pursue a claim via the lengthy and costly process of the European Court of Human Rights in Strasbourg.

Article 8 of the Convention on Human Rights has a significant impact upon Local Authorities and the ways in which they operate. The Article states that:

''everyone has the right to respect for his private and family life, his home and his correspondence''

Essentially, the "public authority" must not in any way interfere with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of any of the following:-

- National Security
- Public Safety
- The Economic well-being of the Country
- The Prevention of Crime and Disorder
- The Protection of Health or Morals
- Protection of the Rights and Freedoms of Others

In addition, any interference with the Article 8 rights should be a proportionate interference in the circumstances.

Since the 5th January 2004 the only ground on which a local authority can now authorise Directed Surveillance is for the purpose of preventing or detecting crime or of preventing disorder. Subsequent changes in legislation now also stipulate that the 'serious crime' test needs to be met; see section 2.7 of this policy.

1.2 Whenever a person undertakes covert surveillance on behalf of a Local Authority, they are placing themselves at risk of breaching Article 8 of the European Convention on Human Rights, unless that surveillance can be justified on the basis that it is conducted in accordance with the law, is necessary for the purpose listed above (ie the prevention or detection of crime or disorder), and is a proportionate action to take.

1.3 The Regulation of Investigatory Powers Act 2000 (RIPA) was passed by Parliament and came into force on the 25th September 2000. This Act regulates covert surveillance and investigations by a number of bodies - including Local Authorities. One of the main purposes of the Act is to ensure that the human rights of any person who is the subject of covert surveillance is protected. However the Act also ensures that law enforcement officers and agencies have the powers they need to do their job properly and to carry out surveillance effectively.

1.4 The purpose of this document is to explain the impact of RIPA upon Denbighshire County Council's procedures in respect of surveillance activity and to provide employees with an understanding of the circumstances where the Act's provisions might apply. This document provides officers with guidance in respect of the procedures that should be followed when covert surveillance is undertaken. This policy should be read in conjunction with the latest Codes of Practice issued by the Home Office and Officers should have regard to the Codes when considering the exercise of their surveillance powers under RIPA 2000. The Codes which are relevant to a Local Authority are:

- Covert Surveillance and Property Interference Revised Code of Practice 2018
- Covert Human Intelligence Sources Code of Practice 2018

Copies of these codes of practice can be obtained from any Authorising Officer listed in chapter 3, from the Councils Legal department or directly from the Home Office website at www.homeoffice.gov.uk

The Council should also have regard to the following revised Procedures:

- Information Commissioner's Code In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information.
- Home Office Surveillance Camera Code of Practice.

1.5 It is important to note that if any covert surveillance work is conducted by the Council and it falls within the provisions of RIPA then the authorisation procedures described in Chapter 3 must be followed before the surveillance occurs. Failure to do so may result in disciplinary proceedings. Obtaining proper authorisation for surveillance will assist in protecting the Council and its officers against complaints of interference with an individual's human rights, and will also protect the admissibility of any evidence gained from such surveillance in a Court of Law.

1.6 Access to Communications Data

In addition, the Council has powers to gain access to communications data. This is information held by telecommunication or postal service providers about the use of their services by persons who are the subject of a criminal investigation. In exercising these powers Officers must have full regard to the Codes of Practice issued by the Home Office:

Code of Practice for the acquisition and disclosure of communications data (March 2015) and Code of Practice for retention of communications data (March 2015) available on www.homeoffice.gov.uk or from the Councils' nominated Single Point of Contract (SPOC).

As for Covert Surveillance, access to communications data must be authorised by a Designated Authorising Officer and obtained via the Councils' SPOC. Specific guidance on these procedures is contained in Chapter 5.

1.7 Encryption

Part 3 of RIPA 2000 came into force in October 2007 to provide a statutory framework allowing all public authorities to require electronic information which they have obtained lawfully or are likely to be obtained lawfully to be put into an 'intelligible form', to acquire the means to gain access to protected information and put that information into 'intelligible form'. For example, where the Council seize a laptop, which may contain protected information that could assist in a prosecution. This is achieved through the assistance of 'NTAC' (National Technical Assistance Centre), who must be approached at the earliest opportunity if the Council are considering the use of these powers. In practice a case is put forward to NTAC, who will provide feasibility and costings of the exercise. NTAC will support the Council in the process to ensure the exercise of these Part 3 powers are undertaken appropriately.

The Investigation of Protected Electronic Information Revised Code of Practice (August 2018) refers to NTAC as the 'guardian and gatekeeper' of the use of Part 3 and any Officer considering the use of these powers should refer to the Home Office Code of Practice available on the Home Office website – www.homeoffice.gov.uk

Specific guidance on these procedures is contained in Chapter 5.

CHAPTER 2: DEFINITIONS OF THE MAIN SURVEILLANCE TECHNIQUES REGULATED BY RIPA

2.1 Surveillance

The Act defines ‘’surveillance’’ as monitoring, observing or listening to persons, watching or following their movements, listening to their conversations or their other activities or communications. It can also encompass recording anything that is monitored, observed or listened to during the course of surveillance. Surveillance may, or may not, be conducted with the assistance of a device.

For example, the installation of CCTV cameras in order to generally observe activity in a particular area will not be ”surveillance” unless the CCTV camera is being used to target a specific person, persons or operation. In cases of uncertainty, officers should seek advice from their department’s Authorising Officers who will in turn consult with the Head of Legal and Democratic Services should they require further clarification or guidance.

2.2 Covert Surveillance

Surveillance will be ‘’covert’’ if it is carried out in a manner calculated to ensure that the person(s) subject to the surveillance are unaware that it is or may be taking place. If surveillance is open and not hidden for the subjects of the surveillance, the surveillance will not generally be covert. Please note that RIPA applies only to covert surveillance so it is vital to consider initially whether or not you are conducting covert surveillance.

2.3 Intrusive Surveillance

This is a form of covert surveillance that is regulated by RIPA.

Intrusive surveillance is defined in the Act as covert surveillance (see 2.2 above) that is carried out in relation to anything taking place on any residential premises or in any private vehicle, and it involves the presence of an individual in the premises or in the vehicle or is carried out by means of a surveillance device.

It is imperative to note that Local Authorities are not empowered by RIPA to carry out intrusive surveillance. If a Local Authority does carry out this type of surveillance, it will be acting beyond the scope of its powers. If you think that your proposed surveillance activity could fall within the definition of ‘’intrusive surveillance’’ you must not proceed with the surveillance. If you need help in determining whether or not you could be conducting intrusive surveillance seek advice from the Head of Legal and Democratic Services.

2.4 Directed Surveillance

This is a crucial method of surveillance which affects Local Authorities. This is surveillance that is covert, but is not intrusive and is undertaken for the purposes of a specific investigation or operation. The surveillance is undertaken in such a manner that it is likely to result in obtaining ‘’private information’’ about a person or persons. Directed surveillance involves the observation of a person or persons with the intention of gathering private information about them to produce a detailed picture of their life, activities and/or,

associates. It will not include entry upon or interference with property, but may include the use of photographic and video equipment (including CCTV).

Before conducting directed surveillance, you need to consider the meaning of ''private information''. Private information will include any information relating to a person's private or family life, and is therefore a very wide definition. The 2000 Act states that private information includes any information relating to a person's private or family life. *Private information should be taken generally to include 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. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly when accessing information on social media or forum type websites.

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 one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purposes of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes surveillance, a directed surveillance authorisation may be considered appropriate.

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

The Covert Surveillance and Property Interference Revised Code of Practice (August 2018) gives practical examples of what is private information and officers may wish to consult pages 15 to 17 of that document which is available on the Home Office RIPA pages of their website.

Use of Social Networking Sites (SNS)

Use of the internet and SNS can provide useful information as part of an Investigation however it is important that these are used lawfully.

It is not possible to provide a definitive list of SNS; but it does include sites such as Facebook, Twitter, LinkedIn, Instagram, YouTube and blogs. It is possible to obtain private information when accessing websites used to advertise goods and services. You must therefore be mindful to the fact that the use of the internate and SNS may potentially mount to directed surveillance and require authorisation.

If you decide it is necessary to access an individual's social networking profile / page in order to take an initial view as to whether there is any substance to an allegation or a matter being investigated; this initial viewing must be reasonable and proportionate. For

example, it would not be reasonable or proporotionate to spend a substantial amount of time searching through the pages of an online profile or to extract and record any material, in the event it may prove useful for your investigation.

Individuals have a reasonable expectation of privacy. Repeated viewing of an individual's online presence or where material is systematically extracted and recorded is likely to require authorisation for directed surveillance irrespective of whether privacy settings are available and applied.

The examples below are taken from paragraph 3.15 of the Covert Surveillance and Property Interference Revised Code of Practice 2018;

Example 1: A police officer undertakes a simple internet search on a name, address or telephone number to find out whether a subject of interest has an online presence. This is unlikely to need an authorisation. However, if having found an individual's social media profile or identity, it is decided to monitor it or extract information from it for retention in a record because it is relevant to an investigation or operation, authorisation should then be considered.

Example 2: A customs officer makes an initial examination of an individual's online profile to establish whether they are of relevance to an investigation. This is unlikely to need an authorisation. However, if during that visit it is intended to extract and record information to establish a profile including information such as identity, pattern of life, habits, intentions or associations, it may be advisable to have in place an authorisation even for that single visit. (As set out in the following paragraph, the purpose of the visit may be relevant as to whether an authorisation should be sought.)

Example 3: A public authority undertakes general monitoring of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends, possible indicators of criminality or other factors that may influence operational strategies or deployments. This activity does not require RIPA authorisation. However, when this activity leads to the discovery of previously unknown subjects of interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation, authorisation should be considered.

Officers should consult paragraphs 3.10 – 3.17 of the revised Code of Practice for Covert Surveillance and Property Interference 2018, for further advice should consult the RIPA Senior Responsible Officer.

Surveillance is directed surveillance if the following are all true:

- It is covert, but not intrusive surveillance
- It is conducted for the purposes of a specific investigation or operation
- It is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation)
- Its is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of the 2000 Act to be sought.
- Thus the **planned** covert surveillance of a specific person, where not intrusive, would constitute directed surveillance if such surveillance is likely to result in the obtaining of private information about that, or any other person.

Please note that directed surveillance would not cover an immediate response to events (eg: detecting something suspicious by chance and continuing to watch). Though in these circumstances applicants must have regard to paragraph 4.17 and the urgency procedures if you *continue* to watch when you ought to have obtained an urgent oral authorisation.

All reasonable alternative methods to resolve a situation such as interview, changing methods of working or levels of security if appropriate for example, should be attempted first.

Where the subject of the covert surveillance is an employee of the Council, subject to the investigation of a criminal matter, the Head of Legal, HR and Democratic Services must be informed.

2.5 Covert Human Intelligence Sources

Covert Human Intelligent Sources (CHIS) is another crucial definition within RIPA which could affect a Local Authority's activities. A person will be a CHIS if he or she establishes or maintains a personal or other relationship with a person for the covert purpose of:

- Obtaining information relating to another person or
- Accessing information about another person, or
- Disclosing information obtained by the use of or as a consequence of such a relationship.

A purpose will be ''covert'' in this respect if the relationship is conducted in such a manner so that one of the parties to the relationship is unaware of the purpose behind that relationship.

An example of this type of surveillance might occur where a professional obtains information about a person without that person understanding the real reason why that information is being collected and without knowing that a professional is seeking to obtain the information in question. This will encompass the use of professional witnesses to obtain information and evidence.

a) Test Purchases

These do not usually require the use of a CHIS because carrying out a test purchase will not usually require the purchaser to establish a relationship with the supplier with the covert purpose of obtaining information. Be aware however, that developing a relationship with a person in a shop to collect information about the seller's suppliers of an illegal product, would involve the use of CHIS.

b) Anti-Social behaviour activities

Persons who complain about anti-social behaviour and are asked to keep a noise log will not normally be a CHIS because they aren't required to establish or maintain a relationship for a covert purpose. (Where the however the complaint is requested to record personal information in the form of a detailed diary, on those carrying out the anti social behaviour, there is the possibility that such persons could be regarded as carrying out directed surveillance, acting as our agents, for which an authorisation

may be required depending on the circumstances. If in doubt, seek advice from the Head of Legal and Democratic Services)

2.6 Persons used as a CHIS

The Council can use a CHIS if RIPA authorisation procedures as detailed in Chapter 3 are followed. However, Officers should always consider whether or not the person to be employed as a CHIS is a suitable person, taking the following into account:-

a) Juvenile Sources

Special safeguards apply to the use of persons under 18 years of age. Only the Chief Executive (or a Corporate Director in the Chief Executive's absence) can authorise the use of a juvenile source. A child under 16 years of age must never be used to give information about his/her parent.

b) Vulnerable Individuals

These are persons who are or may be in need of community care because of age, illness or other disability. Use of such sources should be avoided and in any event, may only be authorised by the Chief Executive (or Corporate Director in the Chief Executive's absence)

It is **not** the Council's normal procedure to recruit a CHIS though it is recognised that some rare circumstances may give rise to this necessity. In these circumstances, Authorising Officers should consider obtaining advice from the Head of Legal, HR and Democratic Services prior to authorisation.

2.7 What you need to do before you undertake any surveillance.....

Before any Council officer undertakes surveillance of any individual or individuals they must first assess whether the activity falls within RIPA.

The following questions may help you decide.....

(a) Is the surveillance ''covert?''

If the investigation and activities are open and are not hidden from the subjects of the investigation then the surveillance will probably not be covert, and the RIPA provisions will not apply. You do not need to obtain authorisation as outlined in Chapter 3 of this Corporate Policy and Procedures if the proposed surveillance is not covert. (See section 2.2 to help you decide this).

(b) Is the surveillance conducted for the purposes of a specific investigation or operation?

Consider CCTV cameras that are regularly visible to anybody walking around a Council office as an example. The cameras will be used to monitor what is generally happening in that Council office and will not be used for the purposes of a specific investigation or operation unless those cameras are used to target a known particular individual and are used to monitor his particular activities.

(c) Will the surveillance reveal private information?

If the surveillance is likely to result in obtaining "private information" (see section 2.4), about a person, RIPA may apply and you will need formal authorisation to carry out that surveillance.

(d) Does the criminal offence that is being investigated punishable, whether on summary (magistrates) or indictment (Crown Court) by a maximum term or **at least 6 months imprisonment, or would constitute an offence under sections 146, 147 or 147A of the Licensing Act 2003 or s.7 of the Children and Young Persons Act 1933 (sale of tobacco and alcohol to underage children)?** If the criminal offence does not meet this criteria, known as the 'Serious Crime Test", then the Council does **not** have the powers to conduct the covert surveillance. Please speak to a legal officer if you have any doubts.

If you have answered ''yes'' to Questions (a) to (d), you will probably be carrying out RIPA regulated surveillance and should therefore seek authorisation as outlined in Chapter 3. If you are unsure as to whether their surveillance will be covert or covered by the Act, you must seek advice from the Head of Legal, HR and Democratic Services before any surveillance is carried out. If in doubt, follow the authorisation procedure outlined in Chapter 3 of this Corporate Policy and Procedures.

CHAPTER 3: PROCEDURES FOR AUTHORISING COVERT SURVEILLANCE

3.1 If, having considered the matters outlined in Chapter 2, you decide that will be conducting surveillance activities covered by RIPA, you must seek authorisation in accordance with the procedures outlined in this chapter. Deciding when authorisation is required involves making a judgement based upon the particular circumstances of each case. If you are in doubt, it is always safer to get authorisation. Alternatively, seek advice as soon as possible from the Head of Legal, HR and Democratic Services.

The Protection of Freedoms Act 2012 now provides that a local authority who wishes to use directed surveillance, acquire communications data or the use of a CHIS under RIPA will need (in addition to an Officer granting authorisation as set out below) to then obtain an order approving the grant or it's renewal, from the Magistrates Court. (a Justice of the Peace, namely a single Stipendiary Magistrate or a Lay Magistrate) before the authorisation can take effect. The standard template for making this application is set out in Appendix 3. The local authority shall following approval by the Authorising Officer, contact the administration team at the Magistrates Court by telephone to arrange a hearing, which shall be in private. A copy of the original RIPA application form duly signed by the AO must be attached. There is further detailed guidance in the Home Office guidance to local authorities in England and Wales on the judicial approval process for RIPA and the crime threshold for directed surveillance (October 2012) available on the Home Office RIPA pages.

Following the changes in 2012 which requires the Council to involve the Magistrates', the effective time is that at which the authorisation is approved by the Magistrate and not the time authorisation is given by the authorising officer.

The decision on who shall appear before the Magistrates is one for the Local Authority; the Home Office guidance expects that it is appropriate for the Investigating Officer to attend as opposed to a Solicitor given they will know most about the matter under investigation, and to keep legal costs down. In respect of applications for Communications Data, the SPOC may attend, subject to any arrangements that are in place with the National Anti Fraud Network (NAFN).

All covert operations should involve a consideration of the health and safety implications involved and an assessment of risk to be undertaken eg such as the need for Investigating Officers to attend in pairs in some circumstances or any necessary precautions which should be in place before embarking on a covert operation. Additionally, the issue of the Council's insurance position may need to be ascertained in advance of the operation.

3.2 The following officers may act as authoring officers for the purposes of RIPA.

Chief Executive only in respect of juveniles/confidential information (or in his/her absence the person acting as the Head of Paid Service)

Corporate Director: Economy and Public Realm

Corporate Director: Communities

s.151 Officer

Monitoring Officer/Senior Responsible Officer only where another Authorising Officer is unavailable to grant an authorisation.

The list may be amended at any time by the Chief Executive and in accordance with The RIPA (Directed Surveillance and CHIS) Order 2010 SI 2010/521. An Investigating Officer should in the first instance attempt to seek authorisation from the Authorising Officer for their department. However if this is impracticable, an authorisation may be sought from any Authorising Officer listed above.

3.3. Authorising Officers should not be responsible for authorising their own activities; however it is recognised that this may sometimes be unavoidable where it is necessary to act urgently. Such instances should however be kept to a minimum. In these circumstances this particular authorisation must be drawn to the attention of the IPCO Inspector and the Central Record will reflect this activity for ease of reference.

3.4 Only the forms found on the Home Office website (RIPA page) can be used for authorisation under this policy. Authorising Officers may authorise covert surveillance only where it is considered necessary in accordance with the relevant purpose of preventing or detecting crime or of preventing disorder and where the extent and nature of the surveillance is proportionate to the aim sought. Authorising Officers will need to be satisfied that any intrusion into an individual's private life can be justified and that the intrusion is essential to the success of an investigation. If the investigation can be furthered without having to resort to covert surveillance techniques, then the use of RIPA should be avoided. It is helpful for applicants to explain what overt measures have been tried or ruled out, before resorting to covert techniques. Authorising Officers should refuse a premature application in these circumstances. In order to ensure that Authorising Officers have enough information to make sensible and informed decisions, officers applying for authorisation should submit a detailed application form to the Authorising Officer..

3.5 Where surveillance is deemed to be necessary, it must be authorised in accordance with the provisions of this Chapter before it is carried out. Proper authorisation should render the Council in a stronger position if challenged on the grounds that it is breached human rights legislation. If authorised and conducted accordingly, the activity is lawful for all purposes (paragraph 27 RIPA)

3.6 Authorising Directed Surveillance

An Authorising Officer will not grant authorisation to an officer to conduct directed surveillance unless he or she *believes* that the authorisation is **necessary** on the relevant ground and also that the surveillance is **proportionate** to the aim sought. Authorising Officers need to have in mind that directed surveillance is an interference with a persons Article 8 rights and that this is only justifiable if it is necessary and proportionate for these activities to take place. If not satisfied, the Authorising Officer must refuse authorisation.

An Authorising Officer must not add to the parts of an application which is completed by the investigating officer or applicant, the content of which must be exclusive to the applicant. The applicant must not in any circumstances complete the parts of the application which is exclusively the Authorising Officer. The applicant's role in the application stops at that part of the form. If further matters are however discussed with the applicant, the Authorising Officer, as a matter of good practice, should mention these discussions in his authorising statement.

The Home Office Code of Practice specifically refers to the following in respect of 'necessity' and 'proportionality':

"If the activities are deemed necessary on one or more of the statutoty grounds, the person granting the authorisation or issuing the warrant must also believe that they are proportionate to what is sought to be achived in carrying them out. This involved balancing the seriousness of the instrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation or warrant will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not alone render the proposed actions proportionate. Similiary, an offence may be so minor that any deployment of covert techniques wqould be disproportionate. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less instrusive means."

The Authorising Officer will therefore carry out a balancing exercise and this needs to be demonstrated on paper, even though the Authorising Officer may well have conducted this exercise in his or her mind. They also may state which matters they personally consider attract greater weight.

The Authorising Officer should take into account the risk that the operation presents to collateral intrusion (intruding upon the privacy of persons who aren't the subject of the investigation). This could affect whether or not an operation is proportionate. The applicant, if collateral intrusion has been identified, must show why the intrusion is in fact justified.

In no circumstances will any covert operation be given backdated authorisation after commencement. Embarking on covert surveillance without authorisation or conducting covert surveillance outside the scope of the authorisation will not provide the protective umbrella of RIPA and may result in disciplinary action being taken against the Officers involved.

The Authorising Officer must set a review date for reconsidering the authorisation, ensure that all forms are completed satisfactorily and that the requirements in 3.8 are complied with. All forms must be submitted to the Head of Legal and Democratic Services department within 3 working days of the authorisation. It is the responsibility of the Authorising Officer, to send the authorisation form, and to consider the most appropriate method of delivery. For high risk operations, where the safety of an individual is concerned, hand delivery may be the only safe and sensible method.

Finally, the **Authorising Officer must allocate a Unique Reference Number** to the application as follows:-

Year/Department/Number of Application - The URN is available from the Head of Legal, HR and Democratic Services' department.

3.7 Equipment

Surveillance equipment will only be installed with the necessary authorisation of the Authorising Officer. The type of equipment used must be documented on the application and also on the Authorising Officer's statement. Those investigating the matter need to be clear what equipment they have authorisation to utilise.

Any surveillance equipment located in occupied residential premises must only be as a result of the express written permission of the tenant or owner occupier.

An inventory of the Council's surveillance equipment is kept by the Authorising Officers of the respective departments. Any purchasing of further surveillance equipment, the respective Authorising Officers must be informed in order for the inventory to be kept up to date.

Any use of this equipment must be documented in the inventory which should make reference to the URN only for security and confidentiality purposes.

Additionally, any surveillance equipment must be kept securely in Council premises.

3.8 Evidence

Any information or recorded evidence will be stored securely and disclosure/access to this evidence will be to those Officers to whom disclosure is necessary such as those Authorising Officers, Investigating Officers and Legal Officers involved in the process or prosecution. Any requests for disclosure to third party agencies will be dealt with via the Authorising Officers, who may seek the advice of the Head of Legal, HR and Democratic Services' department if necessary. Generally disclosure will only be permitted to other law enforcement agencies such as the DWP or the police, to the Subject's legal advisors or to the Subject themselves. Consideration will always be given to the redaction of any third party information, whether written, visual or audio, and also on any possible prejudice to any criminal proceedings, of the Council or another law enforcement agency.

The Data Protection Act 2018 requires the Council to ensure the personal data is stored securely and is not kept for longer than is necessary. See also Chapter 9 of the Covert Surveillance and Property Interference Code of Practice August 2018. Ultimately, it is the Authorising Officer, who owns the product that is obtained, and therefore is responsible for the security of the information.

Tapes and storage

Planning and Public Protection :

Handling Recorded Evidence Obtained by Means of Surveillance

The original recording will be copied, then sealed in an evidence bag and numbered. This will be the 'Master Copy' and handed to the Assistant Head of Service or the Section Manager who will store the 'Master Copy' securely.

The copy disc/tape will become the 'Working Copy' and should this become lost or damaged then application will be made to the Magistrates' Clerk for permission to duplicate the 'Master Copy'. Resealing of the Master Copy will be carried out in front of the Magistrates Clerk.

An entry should be made in the Office Evidence Book for the Master Copy which should include details of the date when handed to the senior officer, together with the identity number on the evidence bag.

The Master Copy should only be removed from storage for production as evidence in court proceedings or as described above.

Where evidence is revealed of an offence and the Authority decide to institute proceedings the following time limits for retention of the recording will apply:

Upon conviction - the recording will be retained for the duration of the case and for two years thereafter.

If no conviction then the recording will be destroyed within 28 days.

Where the Authority decide to offer a formal caution in accordance with Home Office Guidelines, the recording will be retained for two years from the date of the acceptance of the formal caution.

Where it is decided that no formal action will be instituted the recording will be destroyed forthwith, likewise after the expiry of the RIPA where no offence is shown the recording will be destroyed.

Destruction of the recording will be by breaking the disc or cutting it into pieces and an entry made in the Office Evidence Book of the date of destruction and the name of the officer who carried out the destruction.

3.9 Authorising Covert Human Intelligent Sources (CHIS)

When an Authorising Officer is considering authorising the use of a CHIS, he or she must consider the grounds referred to in respect of directed surveillance (3.6 above) and also ensure that arrangements are in place to deal with the following matters:-

- That there is an employee of the Council with day to day responsibility for dealing with the source and for the source's security and welfare (the handler) There must also be a senior officer who has general oversight of the use made of the source, who will in particular have regard for the CHIS safety (the Controller). A full risk assessment must take place, which will be reviewed throughout the recruitment of the CHIS.

- That there is an officer responsible for maintaining a record of the use made of the source

- Consider any adverse impact on Community confidence that may result from the use, conduct or information sought.

- That records disclosing the identity of the source will not be made available to others except strictly on a need to know basis.

Additionally, The RIPA (Source Records) Regulations 2000 (SI 2000/2725) provides for mandatory record keeping in respect of a CHIS :

- The identity of the source
- The identity, where known, used by the source

- Any relevant investigating authority other than the authority maintaining the records
- The means by which the source is referred to within each relevant investigating authority
- Any other significant information connected with the security and welfare of the source
- Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that relevant information has been considered and that any identified risks to the security and welfare of the source have where appropriate been properly explained to and understood by the source
- The date when, and the circumstances in which, the source was recruited,
- The identifies of the persons who will act as handler, controller and person responsible for maintaining records of the use of the source
- The periods during which those persons have discharged those responsibilities
- The tasks given to the source and the demands made of him in relation to his activities as a source
- All contacts or communications between the source and the Council's handler
- The information obtained by the Council by the conduct or use of the source
- Any dissemination by that authority of information obtained in that way
- Any payment benefit or reward made or provided to the source (other than where the source is a council employee acting as an undercover operative).

The Home Office 'Covert Human Intelligence Sources' Code of Practice August 2018 in respect of CHIS provides for the additional records to be kept for the use of CHIS, and Officers are strongly recommended that this Code is referred to when considering the use of a CHIS and throughout the process.

In respect of CHIS whom are juveniles or the mentally impaired, this can only be authorised by the Chief Executive or in their absence a Corporate Director.

3.10 Making sure your authorisations are correct.

As good practice, you should always ensure that each separate authorisation complies with the following points:-

(a) record all applications and approvals for authorisations in writing in the format of the forms available on the Home Office website.

(b) approach each authorisation on an individual basis - apply your mind to the circumstances of the individual case. In respect of Directed Surveillance make full use of the Checklist (at Appendix 1) as you go through the form, if necessary. As a rule of thumb completion of the application form by an Investigating Officer should take at least one hour, given the detail that is required in most cases.

(c) complete one form for each type of authorisation. Distinguish clearly between directed surveillance and covert human intelligent sources and consider whether any collateral intrusion or interference with a privacy of persons other than the subject of a surveillance is likely to arise. You need to describe in the application forms how collateral intrusion is justified in each particular case.

(d) include an assessment of the risk of any collateral intrusion or interference. The Authorising Officer must take this into account particularly when considering whether the surveillance is proportionate to the ends hoped for.

(e) those carrying out surveillance must inform the Authorising Officer if the operation or investigation unexpectedly interferes with the privacy of other individuals who are not the original subjects of the investigation or are not covered by the authorisation. No retrospective application can be made and Investigating Officers should consider the need for a fresh application.

(f) Review authorisations regularly, and diarise dates for expiry and renewals!!! (See chapter 4).

3.11 Confidential Information

Particular care should be taken when any act of surveillance is likely to result in obtaining confidential information. RIPA does not provide for any special protection for confidential material but such information will cover matters subject to legal professional privilege, confidential personal information or confidential journalistic information. Confidential personal information is information that is held in confidence relating to the physical, mental or spiritual counselling concerning an individual (whether living or dead) who can be identified from it.

Please bear in mind that such information is particularly sensitive and that it will be subject to additional safeguards.

Any application for authorisation likely to result in the acquisition of confidential material should include an assessment of how likely it is that confidential material will be acquired. Special care should be taken when the target of the investigation is likely to be involved in handling confidential information. Such applications should only be considered in very exceptional and compelling circumstances with full consideration given to the proportionality issues that it raises. Officers should always seek advice from the Head of Legal, HR and Democratic Services in these instances.

Please note that it is only the Chief Executive (or in his absence, the Acting Head of Paid Service) who is able to act as an Authorising Officer where an operation is likely to result in obtaining confidential information.

3.12 Central Register of Covert Surveillance.

The Head of Legal, HR and Democratic Services will maintain the central register of all requests and authorisations including any request that has been denied by an Authorising Officer. The records in this Central Register will be kept for three years from the date of the authorisation in accordance with the Home Office Code. This record will be made available to the relevant Commissioner or Inspector on request. The central record will also contain, in accordance with the Code of Practice, a copy of the complete application and authorisation. Any subsequent renewal, review or cancellation must also be submitted.

The Head of Legal, HR and Democratic Services must be informed by email in advance that a RIPA form is to be dispatched to the Central Record. All RIPA forms must be sent to the Head of Legal, HR and Democratic Services department within 3 working days of authorisation being granted. The receipt of the RIPA form must be acknowledged by the Head of Legal, HR and Democratic Services department by email. The Central record will be updated upon receipt from the information contained on the form.

The sender must consider the most secure method of delivery of the RIPA form in line

with the type of surveillance and risk. Eg a major joint covert surveillance operation with another enforcement agency, where hand delivery of the form would be appropriate. The documents must be secure and marked private and confidential.

In respect of joint operations with other agencies, one party will lead on obtaining the authorisation, but all the parties will need to see the detail of the authorisation. (R v Sutherland). Those carrying out the investigation, need to be aware of the limits of an authorisation.

3.13 Internal Oversight Arrangements.

The Head of Legal, HR and Democratic Services will be responsible for the monitoring of the authorisations, renewals, reviews and cancellations. Monitoring will take the form of a random selection of forms quarterly, using the Quality Assurance Checklist as a basis. In addition, the Head of Legal, HR and Democratic Services will consider the lawfulness of the authorisation, in particular the necessity and proportionality issues upon receipt of each form, whilst the information required for the central record is inputted.

The outcome of the monitoring will be reported mid year in a short report with the Head of Legal, HR and Democratic Services producing a more detailed Annual Review Report. The Annual Review Report will be reported to the Council's Corporate Governance Committee by the Monitoring Officer/RIPA Senior Responsible Officer.

CHAPTER 4: DURATION, REVIEW AND CANCELLATION OF AUTHORISATIONS

4.1 Authorising directed surveillance or the use of a CHIS is not a decision that should be taken lightly - it is after all, surveillance that interferes with people's privacy. On that basis, a regular review of authorisations must be carried out in order to assess the need for such surveillance to continue. The results of reviews should be kept and recorded safely.

4.2 Please note that there are time limits upon the length of any authorisations granted under RIPA. The length of authorisation will depend on the type of surveillance activity involved:

(a) Directed Surveillance - in all cases 3 months from the date the authorisation should be given, or the date of the latest renewal **. Please not that since the changes introduced in 2012 and the involvement of the Magistrates', the effective time is that at which the authorisation is approved by the Magistrates and not the time authorisation is given by the authorising officer.** Directed Surveillance authorisations do not expire. Under s.45 there is a requirement on the person granting or renewing an authorisation to cancel if he is satisfied that the relevant requirements are no longer satisfied. Even where you believe the authorisation is needed for the full statutory 3 months, the authorisation still needs to be cancelled, it will not expire at the end of the 3 months. On this point the Surveillance Commissioners are very clear. Therefore grant each application for 3 months, then set a review date to cancel or renew during this 3 month time limit. If the evidence is obtained prior to the renew date and no further directed surveillance is necessary, the authorisation must be cancelled.

(b) CHIS - 12 months from the date the authorisation was given, or the date of the renewal. Urgent oral authorisations last initially for 72 hours. In the case of a vulnerable individual eg a juvenile the duration will be for a maximum duration of four months from the time of grant or renewal and the authorisation should be subject to at least monthly reviews.

4.3 All authorisations must be cancelled either when they are no longer necessary or proportionate.

CHAPTER 5 ACCESS TO COMMUNICATIONS DATA and THE INVESTIGATION OF PROTECTED ELECTRONIC INFORMATION .

5.1 Access to Communications Data

Local Authorities can acquire limited information in respect of subscriber details and service data. It does NOT allow Local Authorities to intercept, record or otherwise monitor communications data. **The sole grounds to permit access to communications data, for a Local Authority, is for the purposes of either "preventing or detecting crime, or of preventing disorder".**

Communications data' embraces the 'who', 'when' and 'where' of a communication but not the content - not what was said or written. It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication, including text, audio and video

A strict necessity test must be applied before any consideration is given to requesting communications data. **Any application must be legal, necessary** (a last resort) **& proportionate**. 'Proportionate' includes 'collateral intrusion', as the data provided may invade a third parties' privacy and should, so far as is possible, be minimised.

The overall responsibility for obtaining communication data rests with the Senior Responsible Officer (SRO), who is the Head of Legal, HR and Democratic Services

A Designated Person (DP), who authorises a communication data application must be, at least, a Service Manager

A Single Point of Contact (SPoC) must be accredited by the Home Office, after undergoing accredited training & have proved their compentency, by exam. The Council currently uses the National Anti-Fraud Network for this aspect of investigation.

CSPs (Communication Service Providers) have access to the Home Office's relevant database of accredited SPoCs to ensure the validity of any Notice to provide data.

Procedure for obtaining telecommunications data

Applications to obtain telecommunications data must be submitted to a Home Office accredited Single Point of Contact (SPOC). The Council uses the services of NAFN (the National Anti-fraud Network) for this purpose.

Officers may make the application by accessing the NAFN website. They must therefore be appropriately registered on the NAFN website.

There are full instructions on how to submit an application in the Guidance Manual on the NAFN website. In addition, NAFN have produced a "RIPA Toolkit" for registered users.

The application will first be vetted by NAFN for consistency, before being forwarded by NAFN to the Council's Designated Persons for the purposes of approving the online application.

The Council's Designated Persons are the Public Protection Manager and the Trading Standards Manager. In the future, these roles may be extended (or limited to) Corporate Directors, CEO, and the Council's Monitoring Officer. NAFN will inform the Designated Persons jointly once the application is ready to be reviewed by the Designated Persons.

The relevant Designated Person will then access the restricted area of the NAFN website using a special code, in order to review and approve the application. When approving the application, the Designated Person must be satisfied that the acquiring of the information is necessary and proportionate.

Approvals are documented by the Designated Person completing the online document and resubmitting it by following the steps outlined on the site by NAFN. This online documentation is retained by NAFN who are inspected and audited by the IOCCO.

When submitting an online application, the officer must also inform their Team Manager AND the Designated Person (if different), in order that the Director is aware that the NAFN application is pending.

Acquisition & Disclosure of Communications Data

More information for officers is available in the document "*Guidance for Applicants & Designated Persons Considering Necessity & Proportionality*", produced by the Data Communications Group, is available on the Home Office's website

Although the Council subscribes to NAFN, officers may wish to familiarise themselves with the Home Office 'Acquisition and Disclosure of Communications Data' Code of Practice and Retention of Communications Data Code of Practice March 2015.

http://www.homeoffice.gov.uk/publications/counter-terrorism/ripa-forms/code-of-practice-acquisition?view=Binary

5.2 Encryption – the investigation of protected electronic information.

The power under s.49(1) of RIPA describes the means by which protected information has come into the possession of any person within a public authority. This is likely to include as regards the Council, protected information obtained under an authorisation under Part 2 of RIPA 2000, under Chapter 1, Part 2 of RIPA 2000 (communications data), or obtained by the Council in the exercise of their statutory duties.

Specifically, the provisions of these Part 3 powers are:

- Power to require disclosure of protected information in an intelligible form. (s.49)
- Power to require disclosure of the means to access protected information. (s.50 (3) (c)
- Power to require disclosure of the means of putting protected information into an intelligible form (section 50 (3)(c)

No person can seek to obtain appropriate permission until the approval of the National Technical Assistance Centre has been obtained. NTAC should be consulted in the first instance by email on ripaii@ntac.gsi.gov.uk

Permission will not be granted by the permission, cannot give permission unless the protected information has been obtained lawfully.

CHAPTER 6: CCTV

6. 1 The Covert Surveillance and Property Interference revised Code of Practice (August 2018) at paragraph 3.39 states: *Where overt CCTV, ANPR or other overt surveillance camerars are used in a covert and pre-planned manner as part of a specific investigation or operation, for the surveillance of a specific person or group of people, a directed surveillance authorisation should be considered. Such covert surveillance is likely to result in the obtaining of private information about a person (namely a record of their movements and activities) and therefore falls properly within the definition of directed surveillance .The use of the CCTV, ANPR or other overt surveillance camers in these circumstances goes beyond their intended use for the general prevention or detection of crime and protection of the public.*

6.2 The CCTV control room may on occasions be asked to carry out covert surveillance on behalf of the Council's or other law enforcement agencies, usually the police. This will be in accordance with the protocol the Council has with the police. Such requests to carry out directed surveillance must be supported by a RIPA authorisation, signed by an Authorising Officer, from the enforcement agency concerned and provided to the Council's CCTV Superintendent. It is the Authorising Officers statement that the Councils CCTV control room will require, if the other law enforcement agency do not wish for reasons of confidentiality, to provide the full details of the investigating officers application to the control room staff. For example it is not usually essential that the CCTV be provided with the personal information of the subject under surveillance, it is the scope of the actual surveillance itself that is essential. A copy of the original (whether or not redacted) is acceptable either in person or via the agency email.

The CCTV control room manager shall be provided with copies of any review or cancellation of any authorisation, this includes any Council or other law enforcement agency authorisations, subject to any redactions that the enforcement agency wish to make such as personal information.

This requirement will not apply if the directed surveillance is an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought.

6.3 In respect of applications from internal Council services to conduct covert surveillance via CCTV, the same process shall be followed as if the enforcement agency were external. No covert surveillance shall take place unless the CCTV control room personnel have sight of a copy of the original signed authorisation (redacted if necessary) and a copy of the Magistrates Order signing off the authorisation (again this may be redacted).

6.4 Copies of any authorisations (redacted or otherwise) shall be retained securely in line with the Data Protection Act 2018 at the CCTV control room and retained in accordance with Home Office retention guidelines and this policy.

6.5 You should familiarise yourself with the Home Office Surveillance Camera Code of Practice and the Information Commissioner's code ("In the Picture – A Data Protection Code of Practice for Surveillance Cameras and Personal Information"). Copies available from the Council's Legal Department.

CHAPTER 7: SCRUTINY AND COMPLAINTS.

7.1 The Investigatory Powers Commissioner's Office (IPCO) has a duty to review the exercise and performance of Council departments in respect of their activities under RIPA. The IPCO will regularly inspect the Council in order to ensure that it is complying with statutory functions and duties. This will include scrutiny of authorisations of directed surveillance and CHIS and some activities relating to the investigation of protected electronic information. The latter activity is also overseen by the Interception of Communications Commissioner in part, who will also oversee activities carried out under the Access to Communications regime.

7.2 An Investigatory Powers Tribunal has been established in order to consider complaints made under the 2000 Act. The Tribunal is empowered to order bodies who breach the provisions relating to covert surveillance to pay compensation. Claims must be bought within one year of the alleged breach, although there are provisions which enable the tribunal to extend that period. A person may also complain to the Investigatory Powers Tribunal whose address is:-

Investigatory Powers Tribunal,
PO Box 33220,
London
SW1H 9ZQ.
Tel: 0207 0353711

7.3 Any person who reasonably believes they have been adversely affected by any surveillance activity carried out by on behalf of the Council may either complain to the Monitoring Officer of the Council who will then investigate the complaint, or make a complaint of maladministration to the Ombudsman.

7.4 Clearly, any form of sanctions exercised against the Council, could result in damaging the County Council's reputation and generate adverse media publicity. This is quite apart from any financial implications that could arise. On that basis, it is imperative that all Officers are familiar with the possible (and quite serious) implications that could arise if the guidance offered by this Policy isn't adhered to.

7.5 The Legal, HR and Democratic Services department, additionally report the Council's use of these powers at least annually to the Council's Corporate Governance Committee in order to ensure that the powers are being used consistently and that the policy remains fit for purpose.

This policy will be reviewed no later than January 2024

APPENDIX 1.

REGULATION OF INVESTIGATORY POWERS ACT 2000

Direct Surveillance Form – Quality Assurance Checklist

√

1. Has the application been allocated a Unique Reference Number? Is this inserted on all pages? □

2. Are the full details of the Investigating Officer, Investigation Name (if applicable) and Authorising Officer inserted on page 1? □

3. Does Box 2 (page 2) contain a full, clear explanation of the nature of the investigation and the intelligence that has led to it? Would a person with no prior knowledge of the case understand what this investigation is? If possible include relevant legislation that gives you the power to prosecute or duty to carry out the investigation. □

4. Does Box 3 (page 2) contain a detailed description of the surveillance to be undertaken and the equipment to be used? □
ie what is going to be done? Who is going to do it? Where they are going to do it? When they are going to do it? How they will do it? Eg specific times/public or private vehicle/type of equipment/staff involved etc. Investigating Officer to consider (if appropriate) attaching a plan/map providing the Authorising officer with the full picture.

5. Does Box 4 (page 2) provide the names, addresses and dates of birth (if known) of the subjects of the surveillance? *If you do not know the identity say so.* □

6. Does Box 5 (page 2) explain in sufficient detail what the desired outcome of the surveillance is? □

The Investigating Officer should include all the separate pieces of information hoping to be obtained eg where the offender is dumping illegal waste, who it is that employs him and when this is taking place.

7. Box 6 – The only purpose Local Authorities can now use is the 'prevention or detection of crime or of preventing disorder' <u>All</u> other grounds must be deleted.
Is this the only purpose stated in this box? □

8. Does Box 7 (page 3) explain why the surveillance is necessary? Provide detail of other means of obtaining the evidence that have been tried? Does it explain why overt surveillance is inadequate? □
Factors to include will be: the specific offence, its seriousness, any other evidence you have that links the target with the offender which requires corroboration through surveillance.

9. Does Box 8 (page 3) identify who else may be affected by surveillance (collateral intrusion) & explain the steps taken to minimise this? Even if you cannot minimise you need to show you have considered it. □

10. Does Box 9 (page 4) describe how the surveillance is proportionate, when balanced against the desired outcome? ie balance the intrusiveness on the target and others against the need for the activity in operational terms. Does it say why the desired outcome cannot be achieved in a less intrusive way? □
Demonstrate proportionality by showing you have considered:
- *Can you use less intrusive/overt methods?*
- *Other means used already?*
- *What could be done to lessen the impact on the target eg the amount of information to be gathered, the way the surveillance is carried out, the impact of surveillance on the subject, timing etc.*

Balance this proportionality against:
- *What the surveillance will achieve?*
- *Nature and seriousness of the offence.*
- *Impact of the offence on the victims and community.*
- *The effect the offences have on the public purse.*

11. Does Box 10 (page 4) identify whether □

'Confidential Information' will be likely to be obtained? Eg where following someone you are likely to end up at a church or GP surgery. *NB If so, this can only be authorised by the Chief Executive and Box 14 (page 6) completed

12. Do Boxes 12 & 13 (page 5) contain the Authorising Officer's full statements as to why they believe the surveillance is necessary & proportionate and give full details of the proposed surveillance. Has the AO considered the application objectively? □

The 5 'W's must be considered – the Investigating Officer needs to be clear what they can and cannot do. The AO may set out matters in the application that they have given particular weight to when considering necessity and proportionality. If the application is unclear and there is insufficient detail the AO should consider rejecting.

13. On page 6, has the Authorising Officer – □

- **signed, dated and completed the authorisation**
- **inserted the date of the first review?**
- **completed the expiry date and time of the authorisation?**

14. On page 17, if this was an urgent authorisation, has the Authorising Officer completed Box 15? □

Completed forms must be sent to Legal Services department within 3 working days of authorisation. If the hard copy is sent consider the most secure form of transit (eg hand delivery if possible) and put the Officer holding the Central Record on notice that the authorisation is being dispatched and confirmation of the URN.

APPENDIX 2

STRICTLY CONFIDENTIAL

Denbighshire County Council RIPA CHIS RISK ASSESSMENT FORM

RISK ASSESSMENT FOR THE USE OF COVERT HUMAN INTELLIGENCE SOURCE
THIS FORM IS TO BE SUBMITTED TO LEGAL SERVICES WITH THE CHIS FORM. ALL CHIS FORMS MUST BE HAND DELIVERED AND NOT SENT IN THE INTERNAL POST

Name of source :

Unique reference number:

Is the identity used by the source different to the above?

CHIS pseudonym

Handler details and date duties commenced:

Controller details and date duties commenced:

Is the source working for any other investigation authority? If so by what identity?

Assess and detail the nature and magnitude of any risk connected with the use of the source:

This will include all considerations including risks to the source personally and operational or ethical risks in using the source :

Detail any arrangements made to minimise the risk:

If the source is under 18 detail the arrangements made to satisfy the RIPA (Juveniles) Order 2000:

Authorising Officers' comments on the above arrangements:

Does the Authorising Officer consider that any identified risks are justified? YES/NO and give details:

Have the identified risks been properly explained to, and understood by the source? YES/NO

Date and circumstances in which source was recruited. Give dates when handler and controller commenced duties and any changes to these.

The following officer will be responsible for recording use of the source:

Has the Authority passed the information by the source to anyone else? Give details.

Has the Source been offered or received payment, benefit or reward? Give details.

Detail the tasks given to the Source:

Detail dates of contact with source and notes of information obtained:

Appendix 3

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

Local authority:.....

Local authority department:.....

Offence under investigation:.....

Address of premises or identity of subject:.....

.....

.....

Covert technique requested: (tick one and specify details)

Communications Data ☐

Covert Human Intelligence Source ☐

Directed Surveillance ☐

Summary of details

.....

.....

.....

.....

.....

.....

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

Investigating Officer:.....

Authorising Officer/Designated Person:.....

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

Address of applicant department:.....

.....

Contact telephone number:.....

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

Local authority reference:.....

Number of pages:.....

ATTACHED TO THIS APPLICATION IS: COPY OF THE ORIGINAL SIGNED RIPA APPLICATION.

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:.....

Having considered the application, I (tick one):

- ☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.
- ☐ refuse to approve the grant or renewal of the authorisation/notice.
- ☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

.....

.....

.....

.....

.....

Reasons

.....

.....

.....

.....

.....

.....

Signed:

Date:

Time:

Full name:

Address of magistrates' court:

Blank page

This page is intentionally left blank