APPENDIX 1

New Forest DISTRICT COUNCIL

Regulation of Investigatory Powers Act 2000 (“RIPA”)

Investigatory Powers Act 2016 (“IPA”)

Protection of Freedoms Act 2012

Human Rights Act 1998

Surveillance Policy

This Policy must be read in conjunction with the Home Office Codes of Practice

RIPA codes - GOV.UK

Communications data: code of practice - GOV.UK

Legal and Information Governance

Document publish date: 27 January 2026

Version number 1

Version	Author(s)	Date	Changes Made
1	Service Manager Legal and Information Governance	27 January 2026 (approved by EMT)	Conversion to new policy template, amalgamation of previous Surveillance and Acquisition of Communications Data Policies, updates.

Contents

1. Introduction

1.1 This policy sets out the statutory framework and procedures, including the relevant responsibilities of New Forest District Council ('the Council') and its officers, which govern the Council's lawful use of covert surveillance, covert human intelligence sources ('CHIS') and acquisition and disclosure of communications data for use in an investigation.

1.2 It is based on the requirements of:

- Regulation of Investigatory Powers Act 2000 ('RIPA'),
- Investigatory Powers Act 2016 ('IPA'),
- Home Office Codes of Practice on Covert Surveillance and Property Interference, Covert Human Intelligence Sources and Acquisition and Disclosure of Communications Data.

  RIPA codes - GOV.UK
  Communications data: code of practice - GOV.UK

- Procedures and Guidance issued by the Investigatory Powers Commissioner's Office ('IPCO').

1.3 The use of covert surveillance, CHIS and the acquisition of service user or subscriber information in relation to communications data is sometimes necessary to ensure effective investigation and enforcement of the law.

1.4 These powers should only be used in **exceptional circumstances**. RIPA requires that local authorities follow a clear authorisation process prior to using these powers.

1.5 Authorisations granted under Part II of RIPA or the IPA are subject to all the existing safeguards considered necessary by Parliament to ensure that investigatory powers are exercised compatibly with the Human Rights Act 1998 ('HRA').

2. Statutory Background

2.1 On 2 October 2000, the HRA came into force. This provides for fundamental rights and freedoms contained in the European Convention on Human Rights to be enforceable in UK Courts and Tribunals.

2.2 Article 8 of the Convention reads as follows:-

> *'Everyone has the right to respect for his private and family life, his home and his correspondence.*
>
> *There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of public safety, for the protection of order, health or morals, or for the rights and freedoms of others.'*

2.3 On 25 September 2000, RIPA came into force. This provides a lawful basis for 2 types of investigatory activity to be carried out by local authorities which might otherwise breach Article 8. The activities are:

- **directed surveillance**;
- covert human intelligence sources ("**CHIS**").

2.4 These surveillance techniques can **only** be authorised under RIPA where the use of the surveillance is necessary for the **prevention or detection of a crime** or (in some cases) for the **prevention of disorder**.

2.5 The IPA 2016 provides a lawful basis for local authorities to **acquire communications** data which was previously obtained through RIPA.

2.6 RIPA and IPA set out procedures that must be followed to ensure the surveillance and obtaining communications data activity is lawful which are set out in this policy.

2.7 All Investigating Officers and Authorising Officers should be familiar with RIPA, this Policy, the **Codes of Practice** issued by the Home Office, and the Procedures and Guidance issued by the IPCO.

3. Terminology

3.1 This section of the policy explains some of the terminology that is used in the context of surveillance activities.

Collateral Intrusion

3.2 Collateral Intrusion is the likely effect of the use of surveillance on the private and family life of persons who are not the intended subjects of the activity.

Confidential Information

3.3 This includes:

- Matters subject to legal privilege: Information relating to communications between a professional legal advisor and their client for the purposes of giving advice, in contemplation of legal proceedings or relating to legal proceedings.

- Confidential personal information: Information which relates to the physical or mental health, or spiritual counselling of a person (living or dead) who can be identified from it. For example, information about medical consultations/medical records.

- Confidential constituent information: Information relating to communications between a Member of Parliament and constituent in respect of constituency matters.

- Confidential journalistic information.

3.4 The Authorising Officer and the person carrying out the surveillance must understand that such information is confidential and is subject to a stringent authorisation procedure.

3.5 Authorisation can only be granted by the Chief Executive (or in their absence the deputy Chief Executive or a Strategic Director) (see **Appendix 1**).

Private Information

3.6 This 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 relationships with others, including family and professional or business relationships. Private information may include personal data, such as names, telephone numbers and addresses.

3.7 Whilst a person may have a reduced expectation of privacy when in a public place, 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. For example, two people holding a conversation on a public street or bus may have a reasonable expectation of privacy, even though they are in a public place.

3.8 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. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. For example, where an officer drives past a restaurant to take a photograph of the exterior, this is unlikely to require authorisation under RIPA, as the officer is not collecting private information. However, if the officer wishes to revisit the restaurant on a number of occasions to try to establish occupancy of the premises, this is likely to result in the obtaining of private information about the occupier, and authorisation for directed surveillance will usually be required.

Private vehicle

3.9 A private vehicle is any vehicle, including vessels, aircraft or hovercraft, which is used primarily for the private purposes of the person who owns it or a person otherwise having the right to use it. This would include, for example, a company car, owned by a leasing company and used for business and pleasure by the employee of a company. This is distinct to vehicles owned or leased by public authorities.

Residential premises

3.10 Residential premises are considered to be so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation.

4. Directed Surveillance

4.1 Directed surveillance is a form of surveillance activity that can be authorised under RIPA.

4.2 Surveillance generally includes:

- monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.
- recording anything monitored, observed or listened to in the course of surveillance.
- surveillance with, or without, the assistance of a surveillance device.

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

4.3 Overt surveillance is surveillance which is not secretive or hidden i.e. it will be carried out openly. It includes surveillance where the subject has been told it will happen.

4.4 Covert surveillance is surveillance carried out in a manner calculated to ensure that subjects of it are unaware that it is or may be taking place.

4.5 Directed surveillance is a type of surveillance activity that can be authorised under RIPA. Directed surveillance is surveillance which is **covert** but **not intrusive** and is undertaken:

- For the purposes of a specific investigation or a specific operation
- In such a manner as 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 as detailed above) and
- It 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 to be sought for the carrying out of the surveillance (for example if an officer happens to spot an offence taking place, they may stop and take

photographs as evidence, without requiring authorisation under RIPA).

4.6 Directed surveillance must also relate to the Council's **core functions** which are its specific public functions, rather than the ordinary functions that any organisation might have, for example HR functions.

4.7 Intrusive surveillance occurs when surveillance:

- is **covert**;
- relates to **residential premises** and/or **private vehicles**; and
- involves the presence of a person in the premises or in the vehicle or is carried out by a surveillance device in the premises/vehicle. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle.

4.8 Intrusive surveillance cannot be carried out or approved by the Council.

4.9 Following the changes to RIPA introduced by The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 a **crime threshold** applies to the authorisation of directed surveillance by local authorities.

4.10 Authorising Officers may not authorise directed surveillance unless it is for the purpose of preventing or detecting a criminal offence AND meets the following:

- The criminal offence is punishable by a maximum term of at least 6 months imprisonment; or
- Would constitute an offence under sections 146, 147, or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1993 (offences involving sale of tobacco and alcohol to underage children) regardless of length of prison term.

4.11 The crime threshold only applies to directed surveillance, not to CHIS or the acquisition of communications data.

Examples

4.12 It is possible to authorise directed surveillance under RIPA for some offences under the following categories which are relevant to the Council's functions:

- Fly tipping
- Benefit fraud
- Dangerous dogs
- Listed building offences

As the courts can impose a maximum term of at least six months' imprisonment.

4.13 Directed surveillance may only be carried out subject to the authorisation, approval at the Magistrates' Court and following the procedures in this policy.

4.14 The Home Office Code of Practice for covert surveillance can be found on the Home Office website at:

Covert surveillance code of practice - GOV.UK

4.15 Where covert surveillance is required but does not meet the RIPA crime threshold, or where it cannot fall under RIPA because it does not relate to the Council's core functions, a non-RIPA directed surveillance application may be made. Further details about surveillance outside of RIPA can be found at **Appendix 3** of this policy.

5. Covert Human Intelligence Sources ('CHIS')

5.1 The conduct and use of covert human intelligence sources (commonly known as an informant) occurs when a person establishes or maintains a personal or other relationship with a person:

- For the covert purpose of using the relationship to obtain information or to provide access to any information to another person (i.e. if and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose) or
- To covertly disclose information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

5.2 The use and conduct of a CHIS may only be carried out subject to the authorisation, approval at the Magistrates' Court and following the procedures in this policy . This applies whether the CHIS is a Council officer or another person who is asked to be a CHIS on the Council's behalf.

5.3 Authorisation for CHIS can only be granted if it is for the purposes of 'preventing or detecting crime or of preventing disorder'.

5.4 If a CHIS is used, both the use of the CHIS and their conduct require prior authorisation.

- Conduct is 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 includes actions inducing, asking or assisting a person to act as a CHIS.

5.5 Local authorities are not permitted to grant a CHIS to undertake criminal activity and no criminal conduct authorisations apply.

5.6 Members of the public who volunteer information to the Council in the ordinary course of business are not CHIS and do not require RIPA authorisation.

5.7 There may be instances where an individual, who covertly discloses information though not tasked to do so may nevertheless be a CHIS in accordance with section 26(8) (c) of RIPA. If they acquired the information in the course of, or as a result of the existence of, a personal or other relationship, they are likely to fall within the definition of a CHIS.

5.8 A relationship could exist even if only a single event takes place. Repetition is not always necessary to give rise to a relationship, but whether or not a relationship exists depends on all the circumstances including the nature of that contact.

Examples:

5.9 The following **will not** be a CHIS:

- A member of the public volunteers a piece of information to the Council regarding something they have witnessed in their neighbourhood. They will not be a CHIS as they are not passing on information as a result of a relationship which has been established or maintained for a covert purpose.

- A person complains about excessive noise coming from their neighbour's house and the Council ask them to keep a noise diary. They will not be a CHIS, as they are not required to establish or maintain a relationship for a covert purpose.

5.10 The following **will** be a CHIS:

- Intelligence received by the Council suggests that a local public house will sell alcohol to minors if they are familiar with them. A person under the age of 18 is engaged and trained by the Council and deployed to attend the licensed premises on a number of occasions and then try and purchase alcohol. In this situation a relationship has been established and maintained for the covert purpose and therefore a CHIS authorisation will be required.

- Without being asked, a person provides regular information to the Council about their neighbours' working hours and income as they believe their neighbour is committing benefit fraud. The person regularly visits their neighbour and engages in conversations about their work for the purpose of obtaining this information and passing it to the Council.

5.11 The use of a CHIS is the manipulation of a relationship to gain information. It is a higher risk covert technique and sufficient resources must be dedicated to the oversight and management of the operation.

5.12 The Home Office Code of Practice on Covert Human Intelligence Sources can be found on the Home Office website at:

Covert Human Intelligence Sources code of practice 2022 - GOV.UK

Vulnerable Individuals/ Juvenile CHIS

5.13 Vulnerable individuals and children (‘juveniles’) require greater care in regard to their safety and welfare when deployed as a CHIS.

5.14 Additional requirements, such as enhanced risk assessments, safeguards and protections, apply to the use of a vulnerable individual or a person under the age of 18 as a CHIS due to their level of understanding and/or age. In addition, the best interests of a child should be a primary consideration when deciding whether to deploy a child as a CHIS, during the operation and (if relevant) after the operation. The Council’s Safeguarding Policy should be considered and/or advice obtained prior to the CHIS application.

5.15 Both vulnerable adults and juvenile CHIS should only be used in exceptional circumstances and subject to the enhanced risk assessment process. Where appropriate, external advice should be sought when undertaking the enhanced risk assessment, for example from someone with relevant professional qualifications such as a social worker or an appropriately trained health professional.

5.16 In both cases authorisation for an application to the Magistrates Court can only be granted by the Chief Executive (or in their absence the deputy Chief Executive or a Strategic Director) (see **Appendix 1**). Any officer contemplating the use of a juvenile or a vulnerable person as a CHIS must seek advice from the Council's Legal Team prior to making the application.

5.17 The use or conduct of a CHIS under 16 years of age **must not** be authorised to give information against their parents or any person who has parental responsibility for them. A juvenile CHIS who is aged 16 or 17 years old should only be deployed to gather information against a relative, their parents or any person who has parental responsibility for them where careful consideration has been given to whether the authorisation is justified in light of that fact. In such instances the rationale must be documented.

5.18 In other cases, authorisations should not be granted unless the special provisions contained in The Regulation of Investigatory Powers (Juveniles) Order 2000 are satisfied. This sets out rules about parental consent, meetings, risk assessments and the duration of the authorisation.

5.19 As with all CHIS activity, where the CHIS is a vulnerable adult or a juvenile, the requirements of the **Covert Human Intelligence Sources revised code of practice** must be complied with.

6. CCTV

6.1 The Council operates a close circuit television system ('CCTV') within certain towns in the New Forest District. Use of this system by the Council or third parties such as the police for directed surveillance would require authorisation under RIPA.

6.2 Overt CCTV cameras which are permanently sited for the purposes of, for example, monitoring public safety will not generally require RIPA authorisation, since the public will be aware that such systems are in use.

6.3 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.

Examples:

- Overt CCTV cameras are used to gather information as part of a reactive operation (e.g. to identify individuals who have carried out flytipping). Such use does not amount to covert surveillance as the equipment was overt and not subject to any covert targeting. Use in these circumstances would not require a directed surveillance authorisation.

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

6.4 If another agency – e.g. the Police – wishes to use the Council's CCTV cameras for one of their investigations, this must be agreed by the Service Manager for Community Safety and Support or Operations Manager (CCTV). A copy of the other agency's RIPA authorisation form must be obtained and the details held with the Council's central register. In such circumstances, as long as there is a Police RIPA authorisation, there is no separate need for one of the Council's Authorised Officers to authorise the use of the cameras.

6.5 The deployment of mobile surveillance cameras is likely to be directed surveillance, requiring authorisation, where the surveillance of a specific person or group of people is intended. Requests for deployable CCTV should be made in accordance with the Council's CCTV Policy.

7. Acquisition and Disclosure of Communications Data

7.1 Communications Service Providers ('CSPs') are organisations that are involved in the provision, delivery and maintenance of communications such as postal, telecommunication and internet service providers but also could include, for example, hotel or library staff involved in providing and maintaining e-mail access to customers. The Council must obtain communications data from CSPs in strict compliance with IPA and the authorisation procedure set out in the policy.

Types of Communications Data

7.2 Communications data, telecommunications data and, postal data are defined in Sections 261 and 262 of IPA.

7.3 Communications data is the 'who', 'where', 'when' and 'how' of a communication and may relate to use of the following services:

- Postal service (anything comprised in or attached to a communication for the purpose of a postal service, for example addresses or markings of the sender or the recipient either in writing or through online tracking).
- Email.
- Landline telephone.
- Mobile telephone.
- Internet.

7.4 Telecommunications data are all communications data held by a telecommunications operator or obtainable from a telecommunications system. Under IPA, there are two types of telecommunication data:

- **Entity Data** - this is data about entities or links between individuals and devices. Entities can be individuals, groups and

objects such as mobile phones, tablets or other communication devices.

Entity data may include:

- names and addresses of subscribers, email or telephone account holders as well as payments made;
- make and model of the device used;
- the connection, disconnection and reconnection of services an individual has subscribed to or may have subscribed to.

Entity data describes or identifies how individuals are linked to devices but does not include information about individual events.

- **Events Data** - this is more intrusive; it identifies or describes events which consist of one or more entities, such as individuals engaging in an activity at a specific point (or specific points) in time.

Events data may include:

- call records;
- location of a mobile phone;
- information which identifies the sender or recipient from data held in the communication;
- timing and duration of a call.

Events data does not include non-communication events such as a change in address or telephone number.

Example of difference between entity and events data

7.5 Where an information check is required about who is the subscriber for a specific mobile number:

- The mobile number would be entity data;

- but if further information is required about the date/time a phone call was made by the subscriber, the location or the duration, this would be classed as events data.

7.6 The legal basis for obtaining events data is different than for entity data and must relate to 'serious crime' as defined in IPA, which is a higher threshold.

7.7 The **Home Office Communications Data Code of Practice** contains a list of examples of events data or entity data.

7.8 The Council is not permitted to make an application that requires the processing or disclosure of internet connection records for any purpose.

7.9 The Council is not able to intercept or obtain the content of communications in any circumstances, for example the details contained within an email, text message or voicemail.

Legal basis for Communications Data Authorisation and Notices

7.10 For the Council, the legal basis for the acquisition and disclosure of communications data is only for the prevention and detection of crime or disorder as set out in s73 and s60A IPA.

7.11 Obtaining events data must, in addition, be for 'a serious crime' defined in section 86(2A) IPA as:

- An offence for which an adult is capable of being sentenced to one year or more in prison;
- Any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;
- Any offence committed by a body corporate, or;
- Any offence which involves, as an integral part of it the sending of a communication or a breach of privacy.

7.12 Care should be taken that the appropriate lawful requirements for the purpose of the investigation are met and the correct authorisation procedure is followed before obtaining the data from communication service providers.

7.13 Acquisition and disclosure of communications data is also overseen by the Investigatory Powers Commissioner's Office (IPCO).

7.14 It is an offence for a person in a public authority knowingly or recklessly to obtain communications data from a telecommunications operator or postal operator without lawful authority under section 11 IPA.

7.15 The Home Office Communications Data Code of Practice can be found on the Home Office website at:

Communications data: code of practice - GOV.UK

8. Online convert activity and use of Social Media

8.1 The internet, and the extent of the information that is now available online, presents new opportunities for the Council to view or gather information which may assist in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public.

8.2 It is important that the Council is able to make full and lawful use of this information for its statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations.

8.3 If the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.

8.4 Where Council officers, or persons acting on the Council's behalf, conducts activity on the internet in such a way that they may interact with others in circumstances where the other parties could not reasonably be expected to know their true identity could require a CHIS authorisation. This applies whether the interaction involves publicly open websites such as an online news and social networking service, or more private exchanges such as messaging sites.

8.5 Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for directed surveillance should be considered.

8.6 The Council's Social Media Policy should also be consulted.

8.7 Activity that does not meet the threshold for RIPA authorisation where private information is obtained will still require consideration of Human Rights issues, balancing the protection of rights with the breach of privacy, necessity and proportionality, as well as compliance with the Data Protection Act 2018.

8.8 Where the RIPA crime threshold is not met, a non-RIPA authorisation may still be required. Further information about non-RIPA can be found at **Appendix 3** of this policy.

Directed Surveillance:

8.9 Depending on the nature of the online platform, there may be a reduced expectation of privacy where information relating to a person or group of people is made openly available within the public domain, however in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity.

8.10 Where information about an individual is placed on a publicly accessible database, for example the telephone directory or Companies House, which is commonly used and known to be accessible to all, they are unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information.

8.11 Individuals who post information on social media networks and other websites whose purpose is to communicate messages to a wide audience are also less likely to hold a reasonable expectation of privacy in relation to that information.

8.12 It is possible that when investigating one individual on social media/the internet you might obtain private information about other individuals not just the specific user on the profiles which are viewed, captured or recorded. These individuals might not even be aware this private information has been made public by the profile/account holder.

8.13 If reasonable steps are taken to inform the public or the subjects that surveillance could take place (where appropriate), the surveillance may be deemed as overt, for which authorisation may not be required.

8.14 If it is necessary and proportionate for an officer to breach access controls covertly, an authorisation for directed surveillance is required.

Example

- Where 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.

- 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.

8.15 In order to determine whether a directed surveillance authorisation should be sought, the following factors should be considered:

- Whether the investigation or research is directed towards an individual or organisation;

- Whether it is likely to result in obtaining private information about a person or group of people;

- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;

- Whether the information obtained will be recorded and retained;

- Whether the information is likely to provide an observer with a pattern of lifestyle;

- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;

- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);

- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

CHIS

8.16 Where someone, such as an employee or member of the public, is tasked by the Council to use an internet profile to establish or maintain a relationship with a subject of interest for a covert purpose, or otherwise undertakes such activity on behalf of the Council, in order to obtain or provide access to information, a CHIS authorisation is likely to be required.

8.17 Where a website or social media account requires a minimal level of interaction such as sending or receiving a friend request before access is permitted, this may not itself amount to establishing a relationship, nor would electronic gestures such as liking a post or following the subject's account as a reaction to information posted publicly. A directed surveillance application will still likely apply.

8.18 A CHIS authorisation should be considered if there is an intention to engage with posts covertly, or liking or following posts could lead to interaction with users. This could occur if an officer covertly asks to become a 'friend' of someone on social media where there is a private group.

8.19 It is not unlawful for an officer of the Council to set up a false identity, but an authorisation for the covert investigation would be required. Full consideration of the potential risks of such an approach should be considered at the outset and regularly reviewed.

Advice should be sought from the Legal Team on the covert use of the internet or social media as part of an investigation.

9. Authorisation Procedures

Directed Surveillance and CHIS

Roles of Investigation and Authorising Officers

9.1 Authorising Officers are responsible for assessing and authorising directed surveillance and the use of a CHIS.

9.2 Investigating Officers apply for authorisation from the Authorising Officers.

9.3 A full list of Authorising Officers and their responsibilities is shown in **Appendix 1**. Authorising Officers must not delegate their powers under RIPA.

9.4 A checklist for the respective duties of the Investigating Officer and the Authorising Officer is set out in **Appendix 2.**

9.5 Only Authorising Officers can authorise directed surveillance and the use of CHIS. All authorisations must follow the procedures set out in the policy. Authorising Officers are responsible for ensuring that they have received RIPA training prior to authorising RIPA activities.

9.6 It is the responsibility of Authorising Officers to ensure that when applying for judicial authorisation from the Magistrates' Court that the principles of necessity and proportionality are adequately considered and evidenced; and that reviews and cancellations of authorisations are carried out as required under this Policy.

Necessity and Proportionality Test

9.7 Directed Surveillance and use of a CHIS can only be authorised if the Authorising Officer is satisfied that the activity is:-

- **in accordance with the law** i.e. it must be in relation to matters that are statutory or administrative functions of the Council, the Council's core functions.

- **necessary** for the purpose of preventing or detecting crime or preventing disorder. This is the only ground available to the Council

for authorising RIPA activity and there is a crime threshold for directed surveillance; and

- **proportionate** to what it seeks to achieve. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person as may be affected) against the need for the activity in investigative operational terms. Any conduct that is excessive as to the interference and the aim of the conduct or is in any way arbitrary will not be proportionate. Serious consideration must be given to identifying the least intrusive method of obtaining the information required.

9.8 Investigating Officers should ask the following questions to help determine whether the use of RIPA is necessary and proportionate:

- why it is believed the proposed conduct and use is necessary for the prevention of crime or the prevention of disorder (as appropriate)
- how the activity to be authorised is expected to bring a benefit to the investigation
- 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
- how and why the methods to be adopted will cause the least possible intrusion to the subject/s i.e. interfere with their rights under the Article 8 of the Human Rights Act, or why the method proposed is justified.
- what other reasonable alternatives or less intrusive methods of obtaining information have been considered and why they have been discounted.

9.9 The risk of collateral intrusion should be risk assessed and what measures must be taken to avoid or minimise it. Particular care must also be taken in cases where confidential information is involved. In this instance, the only Authorising Officer will be the Chief Executive (or in their absence the deputy Chief Executive or a Strategic Director) (see **Appendix 1**)

9.10 The Investigating Officer should take reasonable steps to risk assess and ensure that the person carrying out the surveillance or acting as a CHIS is clear on the scope of the activity, the conduct that is and is not authorised. The Investigating Officer and Authorising Officer should have due regard about how this will be managed during the covert operation.

9.11 Authorising Officers should not be responsible for authorising their own activities i.e. those operations/investigations in which they are directly involved. However, it is recognised that in exceptional circumstances this may sometimes be unavoidable.

9.12 A copy of the completed Home Office application and authorisation form must be forwarded to the Council's Legal Team within one week of the authorisation by e-mail as a scanned document. The Council's Legal Team will maintain a central register of the Council's RIPA activity and a unique reference number will be allocated to each application.

Role and Approval by Magistrates' Court

9.13 There is an additional stage in the process for RIPA Directed Surveillance and CHIS investigatory activities. After the authorisation form has been countersigned by the Authorising Officer, the Council is required to obtain judicial approval for either the authorisation or a renewal of an authorisation.

9.14 The magistrate will have to decide whether the Council's application to grant or renew an authorisation to use RIPA should be approved, and it will not come into effect unless and until it is approved by the Magistrates' Court.

9.15 A separate application should be completed when the Council is requesting judicial approval for the use of more than one of the RIPA surveillance techniques (i.e. Directed Surveillance and CHIS) at the same time.

9.16 In cases where there is collaborative working with another agency, for example, the Police, as part of a single investigation or operation, only one authorisation from one organisation is required. This should be made by the lead authority of that particular investigation. Duplication of authorisation does not affect the lawfulness of the investigation or operation but could create an unnecessary administrative burden. Where the Council is not the lead authority, Council officers should satisfy themselves that authorisation has been obtained, and what activity has been authorised.

9.17 The role of the Magistrates' Court is set out in section 32A of RIPA. This provides that the authorisation, shall not take effect until the Magistrates' Court has made an order approving such authorisation. The matters on which the Magistrates' Court needs to be satisfied before giving judicial approval are that:

- There were reasonable grounds for the local authority to believe that the authorisation was necessary and proportionate.
- In the case of a CHIS authorisation, that there were reasonable grounds for the local authority to believe that:
    - arrangements exist for the safety and welfare of the source that satisfy section 29(5) RIPA;
    - the requirements imposed by Regulation of Investigatory Powers (Juveniles) Order 2000 were satisfied.
- The local authority application has been authorised by an Authorising Officer;
- The grant of the authorisation was not in breach of any restriction imposed by virtue of an order made under the following sections of RIPA:
    - 29(7)(a) (for CHIS),
    - 30(3) (for directed surveillance and CHIS).

The procedure

9.18 Investigating Officers wishing to undertake directed surveillance or use of a CHIS must complete the relevant Home Office application form and forward it to the relevant Authorising Officer. The activity must be authorised before it takes place.

9.19 The following steps should be followed:

- Investigating Officer obtains preliminary legal advice from the Council's Legal Team.
- Investigating Officer completes the relevant Home Office application form.
- Authorisation is sought from the Authorising Officer.
- If the application is approved by the Authorising Officer, the Investigating Officer/ legal representative applies for Judicial approval, creates a court pack and Investigating Officer proceeds to court.
- Investigating Officer organises the directed surveillance or use of a CHIS to take place as set out within the parameters of the Court order.
- Investigating Officer sends copy of Magistrates' Court order to the Legal Team.

Additional Requirements for Authorisation of a CHIS

9.20 A CHIS must only be authorised if the following arrangements are in place:

- there is a Council officer with day-to-day responsibility for dealing with the CHIS (CHIS handler) and a senior Council officer with oversight of the use made of the CHIS (CHIS controller);
- a risk assessment has been undertaken to take account of the security and welfare of the CHIS;
- a Council officer is responsible for maintaining a record of the use made of the CHIS;

- any adverse impact on community confidence or safety regarding the use of a CHIS has been considered taking account of any particular sensitivities in the local community where the CHIS is operating; and
- records containing the identity of the CHIS will be maintained in such a way as to preserve the confidentiality or prevent disclosure of the identity of the CHIS.
- A record of decision for CHIS must be completed which covers the requirements that should be in place for handling a CHIS including juvenile and vulnerable CHIS.

Requirements for Authorisation of Acquisition and Disclosure of Communications Data

Roles

9.21 The rules on the granting of authorisations for the acquisition of communications data are different from directed surveillance and CHIS authorisations and involve three roles within the Council. The roles are:

- Investigating Officer;
- Approved Rank Officer;
- Senior Responsible Officer.

9.22 The two external roles are:

- Single Point of Contact (SPoC) at the National Anti-Fraud Network (NFAN);
- Authorising Officer in the Investigatory Powers Commissioner Office (IPCO).

9.23 **Investigating Officer** - This is the officer involved in conducting an investigation or operation who makes an application in writing for the acquisition of communications data.

9.24 **Approved Rank Officer -** This is the Authorising officer who is aware that the application is being made by the Investigating Officer, and is able to verify to the SPoC at NAFN that the acquisition of communications data is necessary and proportionate for the purpose it is required for before it is authorised externally by IPCO.

9.25 **Senior Responsible Officer** - The Home Office Communications Data code of practice requires that local authorities must ensure that someone of at least the rank of the senior responsible officer (SRO) has overall oversight for obtaining Communications Data and must inform NAFN of nominated officers. The SRO for the acquisition and disclosure of communications data is the Council's Monitoring Officer.

9.26 **Single Point of Contact (SPoC) -** The accredited SPoCs at NAFN scrutinise the applications objectively and provide advice to Investigating Officers and Approved Rank Officers ensuring the Council acts in an informed and lawful manner. If no further work is required by the Council in respect of the application, the SPoC will refer the application to IPCO OCDA on the Council's behalf. SPoC's have received training specifically to facilitate lawful acquisition of communications data and effective co-operation between the Council, IPCO and the communication service providers.

9.27 **Authorising Officer at the Investigatory Powers Commissioners' Office (IPCO) -** Communications Data applications do not require judicial approval as is required for directed surveillance or CHIS under RIPA. The external Authorising Officer at the IPCO scrutinises the application independently and either approves or rejects the application setting out the justification for the decision, taking into account the lawfulness of the conduct, and that the appropriate standards and safeguards have been addressed. All correspondence about the application must be through the SPoC at NAFN.

The procedure for applying for Acquisition of Communications Data

9.28 The procedure is as follows:

- Investigating Officer obtains preliminary legal advice from the Council's Legal Team.

- Investigating Officer creates an application using the Cycomms Web Viewer on the NAFN website.
- SPoC Officer at NAFN triages and accepts the application into the Cyclops system.
- SPoC Officer uses Cyclops to update the application details and completes the SPoC report. As part of this, SPoC checks that the Council is lawfully permitted to obtain Communications Data for the purpose it is required for, determines the conduct such as the type of data needed to achieve the Council's purpose. Where the application is for Events Data, that the legal threshold is met and, in all cases, the conduct is justified based on the seriousness of the offence, the risk of unintended results, the risk of excessive data being obtained, including collateral intrusion, including whether other considerations or recommendations are required. The SPoC liaises with Investigating Officer and Approved Rank Officer if further work is required.
- SPoC sends the application to the IPCO for external approval on behalf of the Council.
- If SPoC receives authorisation from IPCO, SPoC sends request to CSP.
- SPoC receives results back from CSP and returns results to Investigating Officer (the applicant). Investigating Officer accesses the Web Viewer and downloads results.
- Investigating Officer sends details of the investigation, type of data required, whether the application was approved by IPCO and the date for this to the Council's Legal Team who will update the Central Record.

9.29 If the application is refused by IPCO, the Council can either:

- decide not to proceed with the application

- resubmit the application with revisions including the justifications for doing so
- challenge the decision made by IPCP if this is agreed by the SRO. Further guidance from IPCO can be provided.

Completing a Communication Data Application Form

9.30 An application to acquire communications data must:

- state the type of data required e.g., entity or events data; describe the communications data required e.g., the subscriber details linked to a telephone number, email address etc.;
- the timescales or specific date or period of the data that it is required. If the data will or may be generated in the future, the future period is restricted to no more than one month from the date on which the authorisation is granted;
- specify the purpose for which the data is required and set out the legislation under which the operation or investigation is being conducted. This must be a statutory function of the Council for the prevention or detection of crime or preventing disorder (or for events data, this must meet the threshold for serious crime).
  - include a unique reference number;
  - include the name and the office, rank or position held by the person making and verifying the application;
  - describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person or other person relevant to the investigation or operation;
  - include the operation name (if applicable) to which the application relates;
  - explain why the acquisition of that data is considered necessary and proportionate in the circumstances based on

the link between the investigation, the subject or other individuals, and why the specific communication data is required, what other lawful, reasonable or least intrusive methods were considered and why these were rejected;

- present the case for the authorisation in a fair and balanced way taking into account the size and scope of the investigation. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;

- consider and, where appropriate, describe any risk of meaningful collateral intrusion. the extent to which the privacy rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances. For example, where access is for 'outgoing calls' from a 'home telephone' collateral intrusion may be applicable to calls made by family members who are outside the scope of the investigation. The applicant therefore needs to consider what the impact is on third parties and try to minimise it;

- consider and, where appropriate, describe any possible unintended consequences of the application; and

- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject/individual(s) of the fact that an application has been made for their data.

Urgent Authorisations (All covert activity)

9.31 As an authorisation under RIPA is not approved until signed off by a Magistrates' Court, urgent oral authorisations are not available.

9.32 Urgent oral authorisations are also not available for Communications Data.

10. Application Forms

10.1 The link to the Government application forms for Directed Surveillance and CHIS can be accessed from the link below:

RIPA forms - GOV.UK

10.2 For communications data, the application should be made electronically through the NAFN website.

10.3 The person completing the form is responsible for ensuring that the form used is the most up-to-date version

10.4 The forms for applications, renewals, reviews and cancellations should be completed in as much detail as possible.

10.5 Each investigation or operation should be given a unique reference number ('URN') on the application form by the Service Manager Legal and Information Governance. Any reviews, renewals or cancellation forms should be identified by the same URN.

Duration of the Authorisation

10.6 Authorisation/ notice durations are:

- for directed surveillance the authorisation remains valid for **3 months** after the date of authorisation;
- for a CHIS the authorisation remains valid for **12 months** after the date of authorisation (or **4 months** if a juvenile CHIS is used).
- a communications data notice remains valid for a maximum of **1 month**. All authorisations and notices are expected to specify dates and times for the acquisition or disclosure of the information.

10.7 Authorisations should not be permitted to expire; they must be either renewed or cancelled when the activity authorised has been completed or is no longer necessary or proportionate in achieving the aim for which it was originally authorised. This is a statutory requirement which means that **all** authorisations must be reviewed to decide whether to cancel or renew them.

Review of Authorisations

10.8 Authorising Officers must make arrangements to periodically review any authorised RIPA activity. It will be the responsibility of the Authorising Officer to diarise when reviews should be held.

10.9 Officers carrying out RIPA/ IPA activity, or external agencies engaged by the Council to carry out such activity on its behalf, must periodically review and report back to the Authorising Officer/ Approved Rank Officer if there is any doubt as to whether the activity should continue.

10.10 Reviews should take place as often as necessary and practicable, and this will need to be determined on a case by case basis. More frequent reviews should take place where surveillance results in collateral intrusion or access to confidential information.

10.11 Where the nature or extent of the impact of an authorisation becomes greater than that anticipated in the original authorisation, the Authorising Officer should immediately review the authorisation and reconsider the proportionality of the operation.

10.12 For Juvenile CHIS, the CHIS Code of Practice stipulates that the authorisation should be reviewed on a monthly basis.

10.13 All reviews of RIPA activity should be recorded on the appropriate Home Office review form and must be sent to the Council's Legal Team within one week of the review to enable the central record on RIPA to be updated.

Renewal of Authorisations

10.14 If the Authorising Officer/ Approved Rank Officer considers it necessary for an authorisation to continue a renewal may be sought for a further period, beginning with the day when the authorisation would have expired but for the renewal. The Authorising Officer/ Approved Rank Officer must consider the matter again taking into account the content and value of the investigation and the information so far obtained.

10.15 Renewed authorisations will normally be for a period of:

- up to 3 months for directed surveillance,
- 12 months in the case of CHIS,
- 4 months in the case of juvenile CHIS and
- 1 month in the case of a communications data authorisation.

10.16 Authorisations may be renewed more than once, provided they are considered again and continue to meet the criteria for authorisation.

10.17 Applications for the renewal of an authorisation for directed surveillance or CHIS authorisation must be made on the appropriate form and added as an addendum to the application form which granted the initial authorisation.

All directed surveillance and CHIS renewals will require an order of the Magistrates' Court.

10.18 A copy of the Council's notice of renewal of an authorisation must be sent to the Council's Legal Team within one week of the renewal, together with a copy of the Magistrates' Court order renewing the authorisation to enable the central record on RIPA to be updated.

10.19 For communications data, renewals must be made via the NAFN SPoC. The reasoning for seeking renewal of a communications data authorisation should be set out by the applicant in an addendum to the application form which granted the initial authorisation.

Cancellation of Authorisations

10.20 The person who applied for or last renewed the authorisation must cancel it when they are satisfied that the directed surveillance, CHIS or communications data authorisation or notice no longer meets the criteria for authorisation, such as when it is no longer necessary for the statutory purpose or the activity is no longer deemed to be proportionate. For directed surveillance and CHIS cancellations must be made on the appropriate Home Office form.

10.21 Where necessary and practicable, the safety and welfare of the CHIS should continue to be taken into account after the authorisation has been cancelled, and all welfare matters addressed.

10.22 A copy of the Council's notice of cancellation of an authorisation must be sent the Council's Legal Team within one week of the cancellation to enable the central record on RIPA to be updated.

10.23 For Communications Data, the NAFN SPoC must be made aware of the cancellation who will cease the authorised activity, ensure any notices are cancelled and inform the Communication Service Provider.

What happens if the surveillance interferes with the privacy of others?

10.24 Those carrying out the covert surveillance should inform the Authorising Officer if the investigation unexpectedly interferes with the privacy of individuals who are not the original subjects of the investigation or covered by the authorisation. In some cases, the original authorisation may not be sufficient to cover the activity required or information likely to be gathered and, in such cases, consideration should be given as to whether a separate authorisation is required.

11.Errors

11.1 An error should be reported if it is a ‘relevant error’ to IPCO.

11.2 Under section 231(9) of the IPA, a relevant error is an error by a public authority in complying with any requirements that are imposed on it by an enactment, such as RIPA, which is subject to review by a Judicial Commissioner.

11.3 Examples of a relevant error include where surveillance or CHIS activity has taken place without lawful authorisation, and/or without adherence to the safeguards set out within the relevant statutory provisions or the relevant Home Office Code of Practice.

11.4 Where a relevant error has been identified, the Council should notify the IPCO as soon as reasonably practical, and no later than 10 working days (unless otherwise agreed by IPCO).

12.Records and Documentation

Departmental Records

12.1 Applications, renewals, cancellations, reviews and copies of notices must be retained by the Council in written or electronic form, and physically attached or cross-referenced where they are associated with another matter.

12.2 These records will be confidential and should be retained for a period of at least five years from the ending of the authorisation. Where it is believed that the records could be relevant to pending or future court proceedings, they should be retained and then destroyed five years after last use.

12.3 In relation to communications data, records must also be held centrally by the SPoC. These records must be available for inspection by the IPCO and retained to allow the Investigatory Powers Tribunal to carry out its functions.

Central Record of Authorisations, Renewals, Review and Cancellations

12.4 A central record of directed surveillance, CHIS and access to communications data authorisations is maintained by the Council's Service Manager – Legal and Information Governance.

12.5 The central record is maintained securely in accordance with the requirements set out in the Home Office Codes of Practice. This is retained in perpetuity.

12.6 This will contain the following information:

- the type of authorisation
- the URN
- the dates that the authorisation was granted, reviewed, renewed or cancelled.
- details of attendances at the Magistrates' Court to include date of

- attendances, the determining Magistrate, the decision of the Court and the time and date of that decision.
- the name and rank of the Authorising Officer for the initial authorisation and any reviews, renewals or cancellations.
- whether the Authorising Officer is involved in the investigation.
- the file reference for the investigation.
- whether the authorisation was likely to result in the obtaining of confidential material.

12.7 In order to keep the central record up to date, Authorising Officers/Investigating Officers must, in addition to sending through the Home Office application, authorisation form, Magistrates' Court order or IPCO decision documents within one week of the authorisation being approved by the Magistrates' Court or IPCO, send notification (by e-mail) of every renewal, cancellation and review on the Council's notification forms within five working days.

12.8 In relation to the use of a CHIS the Services Manager Legal and Information Governance will also maintain the following documents:

- Any risk assessment in relation to the CHIS.
- The circumstances in which tasks were given to the CHIS.
- The value of the CHIS to the Council.

12.9 Using the information on the central record the Council's legal Team will:

- remind Authorising Officers/Investigating Officers in advance of the expiry of authorisations;
- remind Authorising Officers and Investigating Officers of the need to ensure surveillance or CHIS conduct does not continue beyond the authorised period;
- remind authorising officers and Investigating Officers to regularly review current authorisations

- provide information to IPCO about the use of RIPA and IPA activity when required.

Safeguarding and the Use of Material (including Data protection considerations)

12.10 All material obtained through the use of directed surveillance, CHIS or acquisition of communications data records containing personal data must be handled in accordance with the Data Protection Act 2018 ('DPA') and the Council's Data Protection Policy.

12.11 The data protection principles under the DPA includes that personal data should only be processed if it is fair and lawful to do so, that the data processed are adequate, relevant and not excessive for the purpose it was collected.

12.12 A personal data breach can be broadly defined as a security incident that has affected the confidentiality, integrity or availability of personal data. Care must also be taken that personal data collected as part of an investigation is held in a manner that ensures appropriate security of the data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage.

12.13 A personal data breach may need to be reported to the Information Commissioner's Office within 72 hours of officers becoming aware of the breach

12.14 To mitigate against risk of personal data being compromised, all records and materials should be stored securely; clearly labelled; classified where appropriate as OFFICIAL or SENSITIVE to demonstrate the degree of sensitivity of the information; the appropriate retention period should be recorded at the outset and reviewed.

12.15 The admissibility of evidence is governed primarily by the common law, the Criminal Procedure and Investigations Act 1996, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1984 and the HRA. Ensuring the continuity and integrity of evidence is critical to every prosecution.

12.16 Access to material obtained should be limited to those officers that have a legitimate reason for storing or accessing the records, with appropriate access controls in place. The data should not be stored for any longer than is necessary for any authorised purpose, and thereafter securely destroyed. This applies to all copies, extracts and summaries of the material obtained.

12.17 A record should also be made of all data pathways relating to material obtained through surveillance activities.

12.18 Where an authorisation results in excessive data having been acquired, the data should only be retained where it's appropriate and lawful to do so. The data must be reviewed to determine whether there is an intention to use it, and the reasons for requiring it, including whether retention of the data is necessary and proportionate. Contact the Legal Team if advice is required.

13. Governance, Oversight, and Continuous Compliance

Training and Awareness

13.1 The Service Manager – Legal and Information Governance will arrange regular training on RIPA and the acquisition of Communications Data.

13.2 All Authorising Officers and investigating officers should attend at least one session every two years and further sessions as and when required.

13.3 Any officer contemplating RIPA or the acquisition of Communications Data Should seek advice from the Council's Legal Team in the event of any queries or concerns as to the process.

13.4 The Service Manager – Legal and Information Governance will be responsible, along with the Senior Responsible Officer for raising corporate awareness of RIPA and this Policy.

Monitoring of Authorisations

13.5 The Monitoring Officer is the Senior Responsible Officer in relation to activity under RIPA and IPA and is responsible for:

- the integrity of the process in place to authorise directed surveillance, the use of a CHIS and the acquisition and disclosure of communications data
- compliance with Part II of RIPA, Part 3 of IPA, the relevant Home Office Codes of Practice and this Policy
- oversight of the reporting of errors to IPCO, and the identification of the causes of the errors and implementation of processes to minimise repetition of errors
- engagement with the Commissioner or Inspectors of the IPCO when they conduct inspections, and

- where necessary, overseeing the implementation of any post-inspection plans recommended or approved by the Commissioner
- ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection report prepared by the Commissioner.
- The IPCO has a duty to keep under review the exercise and performance of the Council's use of directed surveillance, CHIS, and the exercise and performance of the Council's use of its acquisition and disclosure of communications data powers. The IPCO will periodically inspect the Council and may carry out spot checks unannounced.

Complaints

13.6 Any person who believes they have been adversely affected by surveillance or other covert activity undertaken by or on behalf of the Council may complain to the Investigatory Powers Tribunal at:

Investigatory Powers Tribunal
PO Box 33220
London
SW1H 9ZQ

Member review

13.7 The Service Manager – Legal and Information Governance will invite members every year through the Audit Committee to review the Council's RIPA Policy for that period to ensure it is fit for purpose. Members will also be provided with an annual update on the Council's use of its RIPA powers.

Policy and Implementation

13.8 This RIPA Policy is operational from { } and replaces any previous policies and procedures relating to RIPA, surveillance or acquisition of communications data.

Appendices

Appendix 1 - Functions that may be undertaken by Authorising Officers

1. Authorise an application for authority to carry out directed surveillance or for the conduct or the use of a CHIS.

2. Review an authorisation to carry out directed surveillance or the conduct or use of a CHIS on or before the specified date.

3. Authorise renewal of an application for authority to carry out directed surveillance or for the conduct or use of a CHIS.

4. Authorise cancellation of an application for authority to carry out directed surveillance or for the conduct or use of a CHIS.

5. Monitor the produce of the surveillance or from the conduct or use of a CHIS.

6. Authorise an application where the likely consequence of directed surveillance or conduct or use of a CHIS would be intrusion on another person other than the target (collateral Intrusion).

7. Authorise an application where the likely consequence of the directed surveillance or conduct or use of a CHIS would result in Council obtaining confidential material.

8. Authorise the use of a CHIS who is a minor.

9. Authorise the use of a CHIS who is a vulnerable person.

RANK/TITLE	**AUTHORISED FUNCTIONS (from numbered list above)**
Chief Executive	1-10
Deputy Chief Executive or a Strategic Director	1-7 (8,9, 10 in Chief Executive's absence)
Service Managers for: Development Management Environmental & Regulation Revenues, Benefits & Customer Services Public Realm & Sustainability Community Safety & Support Housing Resident Services	1-7

Appendix 2 Application and Authorisation Checklist

Investigating Officer must:

Read the Surveillance Policy document and be aware of any other relevant guidance.	
Determine that directed surveillance and/or a CHIS is required.	
For directed surveillance, assess whether the authorisation will be in accordance with Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 and be able to demonstrate that the suspected offence is subject to a custodial sentence of 6 months or more or that the surveillance is in connection with the sale of alcohol or tobacco to children.	
Assess whether authorisation is necessary under RIPA and whether the surveillance could be done overtly.	
Consider whether surveillance will be proportionate.	
Consider all less intrusive options which may be available and practicable and use that option first.	
If authorisation is necessary and proportionate, request a URN from the Service Manager Legal and Information Governance, prepare and submit an application to carry out directed surveillance or conduct or use of a CHIS to an Authorising Officer.	
REVIEW REGULARLY and submit to Authorising Officer on date set.	
If operation is no longer necessary or proportionate, complete cancellation form and submit to Authorising Officer.	

Authorising Officer must:

Consider in detail whether all options have been duly considered, including taking into account the Surveillance Policy document and any other relevant guidance.	
For directed surveillance, confirm that the offence is subject to a custodial sentence of 6 months or more or the surveillance is in connection with the sale of alcohol or tobacco to children.	
Consider whether surveillance can be considered to be in accordance with the law and is necessary and proportionate to the offence being investigated.	
Authorise only if an overt or less intrusive option is not practicable.	

Ensure the relevant judicial authority has made an order approving the grant of the authorisation.	
If surveillance is necessary and proportionate: • Review authorisation • Set review timetable	
Cancel authorisation when it is no longer necessary or proportionate.	

Appendix 3 Non-RIPA Guidance

1.1 Non-RIPA directed surveillance is covert surveillance:

- which does not meet the 'crime threshold' under RIPA 2000/ or the core function test and
- does not require external authorisation as under RIPA but instead requires internal authorisation.

1.2 Examples of non-RIPA surveillance could apply to matters which relate to civil matters such as some licensing matters, planning, safeguarding, immediate response surveillance or noise/anti-social behaviour investigations, debt recovery or matters where the RIPA lawful basis and 'crime threshold' (where relevant) is not met.

1.3 It must be noted that non-RIPA covert surveillance activity should only be undertaken where there is a lawful basis for doing so under Article 8 of the European Convention of Human Rights as set out in the HRA.

1.4 The use of non-RIPA should only be in exceptional circumstances and in line with the RIPA guidance set out for directed surveillance in this policy, and/or the use of a CHIS (where applicable). This includes the use of the internet and social media as part of covert investigations; further advice about the use of social media as part of investigations can be provided from the Legal Team if required.

1.5 The use of non-RIPA covert activity is high risk. If non-RIPA surveillance or other activity is deemed unlawful or not authorised or monitored correctly, the Council could be at risk of being the subject of complaints, the matter investigated by the Local Government and Social Care ombudsman, or result in legal or other action taken against the Council; all of which may result in reputational damage.

1.6 Case law has set out that the factors and procedure for non-RIPA surveillance should mirror the requirements under RIPA 2000 and the

Home Office statutory code of practice for covert surveillance as far as practicable.

1.7 This means that the Council is not permitted to undertake intrusive surveillance and higher levels of authorisation may be required for certain types of surveillance (e.g. obtaining certain types of confidential information).

1.8 Only Authorising Officers should authorise non-RIPA applications and renewals.

1.9 Investigating Officers should consult with the Council's Legal Team for preliminary advice on all proposed non-RIPA activity.

1.10 Investigating Officers and Authorising Officers should use the relevant RIPA forms which can be found on the intranet and mark these clearly as 'Non-RIPA directed surveillance'. Advice about completing the forms can be obtained from the Legal Team.

1.11 All non-RIPA Applications, authorisations, renewals and cancellations should be sent to Legal Team so that a record can be made on the central record. Where the use of the internet and social media is required as part of the investigation, the reasons for why the use of social media is required, how this will be undertaken, and the arrangements expected to be in place should be set out clearly.

1.12 Where the investigation may require a CHIS operative to set up or maintain a covert relationship for the purpose of obtaining information covertly or disclosing information which was obtained through such a relationship, a non-RIPA CHIS application may be required in addition to a non-RIPA directed surveillance application.

1.13 Applicants and Authorising Officers must be satisfied that covert activity under non-RIPA is lawful, necessary and proportionate in accordance with Article 8 of the ECHR as set out under the HRA.

1.14 The time period for authorisations and renewals should mirror the requirements under RIPA. Authorisations and renewals should not be allowed to expire.

1.15 Applicants must ensure all appropriate steps are taken to safeguard the material and that access to the information is on a 'need to know basis'. Where personal data is being processed, for example, the, use, handling and retention of materials, applicants must comply with all relevant data protection laws.