Regulation of Investigatory Powers Policy and Guidance

USE OF DIRECTED SURVEILLANCE
USE OF HUMAN INTELLIGENCE SOURCES
OBTAINING COMMUNICATIONS DATA

Date Policy Approved: 19 January 2022

Approved by: Cabinet

Date of Implementation: 1 February 2022

Contents

PART A Introduction & RIPA General

1. Introduction

1.1 The primary aim of Central and Local Government enforcement is to protect the individual, the environment and a variety of groups such as businesses, consumers and workers. At the same time, carrying out enforcement functions in a fair, practical and consistent manner helps to grow and promote a prosperous and thriving national and local economy. Shropshire Council (the Council) is committed to these aims and to maintaining a fair and safe society.

1.2 The performance of certain investigatory functions to fulfil the Council's statutory duties and ensure regulatory compliance may require the Council to undertake covert techniques that involve the surveillance of individuals, the use of undercover officers and informants or obtaining communications data. Such actions may intrude on the privacy of individuals and can result in private information being obtained and, as such, should not be undertaken without full and proper consideration. The Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) govern these activities and provide a means of ensuring that they are carried out in accordance with the law and subject to safeguards against abuse.

1.3 Within the Council, the service areas/functions that are likely to undertake investigations include, but are not limited to, trading standards, licensing, environmental health, planning, building control, environmental maintenance, education welfare, housing, social care, council tax, benefits, rights of way, human resources and internal audit. All these service areas/functions may need to use covert techniques as part of their official duties to effectively deliver service and Council outcomes.

1.4 All surveillance activity can pose a risk to the Council from challenges under the European Convention on Human Rights (EHCR) and the Human Rights Act 1998 (HRA). All staff involved in the process must, therefore, take their responsibilities seriously, which will assist with the integrity of the Council's processes, procedures and oversight responsibilities.

1.5 In preparing this Regulation of Investigatory Powers Policy and Guidance (the Policy) the Council has followed the RIPA and IPA Codes of Practice (the Codes) and the Office of Surveillance Commissioners (OSC) Procedures and Guidance 2016.

1.6 The Council's governance structure for the purposes of RIPA and IPA is set out at **Appendix A**.

1.7 The officers designated for the purposes of RIPA and IPA and referred to by role within this Policy are set out in **Appendix B**.

1.8 The application and authorisation process is set out in **Appendix C**.

1.9 If having read this Policy any matter is unclear, advice should be sought from the Council's RIPA Coordinator or one of the designated Authorising Officers (AO).

2. Scope of Policy

2.1 The purpose of this Policy is to ensure there is a consistent approach to the authorisation and undertaking of surveillance activity that is carried out by the Council. This includes the use of undercover officers and informants, known as Covert Human Intelligence Sources (CHIS), and obtaining communications data. This will ensure that the Council complies with RIPA and IPA.

2.2 The Policy is intended to demonstrate that covert techniques will only be used to obtain information or evidence when no other investigation method or technique will deliver the required outcomes.

2.3 All residents and businesses within Shropshire will benefit from this Policy as it provides the framework to ensure compliance with RIPA and IPA and thus ensures human rights are protected when undertaking investigatory functions; in particular, it sets out how the Council intends to limit intrusion into the personal activities of individuals. The Policy assists the Council to identify and take the appropriate investigatory action to reduce the level of crime in the community.

2.4 The Policy provides guidance on the directed surveillance and CHIS authorisation processes and the roles of the respective staff involved

2.5 The Policy sets out the approach to be taken to ensure that all online research and investigations are conducted lawfully and ethically to reduce risk. It provides guidance to all staff within the Council, when engaged in their official capacity, of the implications and legislative framework associated with online internet and social media research. It also ensures that the activity undertaken, and any evidence obtained will stand scrutiny.

2.6 The Policy provides guidance on surveillance which needs to be undertaken by the Council but cannot be authorised under RIPA. This type of surveillance must be compliant with the ECHR/HRA.

2.7 The Policy takes account of and identifies the cross over with other policies, legislation and guidance, particularly with the HRA, the Data Protection Act 2018 (DPA), the General Data Protection Regulations (GDPR), the Criminal Procedure and Investigations Act 1996 (CPIA) and the National Police Chiefs Council (NPCC) Guidance on Open Source Investigation/Research.

2.8` The Policy does not provide detailed guidance with respect to obtaining communications data. Officers must refer to the Communications Data Code of Practice, specifically the Local Authority Procedures in section 8.

2.9 All RIPA covert activity must be authorised and conducted in accordance with this Policy, RIPA, IPA and the Codes and any other relevant legislation, policies and guidance referred to within this document. All officers involved in the process must have regard to this Policy and the statutory Codes issued under section 71 of RIPA for both directed surveillance and the use of CHIS and section 241 of IPA in relation to obtaining communications data. The Codes are available here.

2.10 A failure to adhere to this Policy may result in staff being dealt with through the Council's disciplinary procedure.

2.11 The Policy is not exempt from disclosure under the Freedom of Information Act 2000.

3. Background to RIPA and IPA and Lawful Grounds

3.1 When the HRA came into force, it potentially made it unlawful for the Council to breach any article of the ECHR.

3.2 Article 8 of the ECHR states that: -

(a) Everyone has the right of respect for his private and family life, his home and his correspondence.

(b) There shall be no interference by a Public Authority with the exercise of this right except such as in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health and morals or for the protection of the rights and freedoms of others.

3.3 The right under Article 8 is a qualified right and the Council is permitted to interfere with this right for the reasons given in 3.2 (b) above if it is necessary and proportionate to do so.

3.4 Those who undertake directed surveillance, CHIS activity or obtain communications data on behalf of the Council may not breach an individual's human rights unless such surveillance is **lawful,** consistent with Article 8 of the ECHR and is both **necessary** (see section 45) and **proportionate** (see section 46) to the matter being investigated.

3.5 RIPA and IPA provide the legal framework for lawful interference to ensure that any activity undertaken, together with the information obtained, is ECHR/HRA compatible.

3.6 The Council can only authorise directed surveillance for the purpose of preventing or detecting conduct which constitutes a criminal offence which is punishable (whether on summary conviction or indictment) by a maximum term of at least six months' imprisonment (the directed surveillance serious crime threshold); or involves the sale of alcohol or tobacco to children (see section 14).

3.7 The Council can authorise a CHIS for the purpose of preventing and detecting crime and preventing disorder and the offence does not have to be punishable by a maximum term of at least six months' imprisonment.

3.8 The Council's authorisation for either directed surveillance or CHIS activity can only take effect once an Order approving the authorisation has been granted by a Justice of the Peace (JP).

3.9 With respect to communications data, the Council can only obtain events data[1] for the purpose of preventing or detecting serious crime[2] and, for any other type of communications data, for the purpose of preventing or detecting crime or of preventing disorder.

[1] Events data - refer to the telecommunications definitions in IPA at section 261
[2] Under IPA, the definition of 'serious crime' differs to that under RIPA. Refer to IPA sections 86(2A) and 263(1) for further details.

3.10 The authorisation process for communications data must be undertaken through the National Anti-Fraud Network (NAFN). Verification of applications must be undertaken by the Council's Authorising Officers (AO). The Council's Senior Responsible Officer (SRO) must be aware that such applications are being made before they are submitted to the Office for Communications Data Authorisations (OCDA). NAFN is responsible for submitting applications to the OCDA on behalf of the Council.

3.11 The Council may not make an application to obtain communications data that requires the processing or disclosure of internet connection records for any purpose.

3.12 RIPA ensures that any surveillance conduct which is undertaken following the correct authorisation and approval from a Justice of the Peace and, where communications data is obtained under IPA and undertaken through NAFN and OCDA, is lawful. These processes protect the Council from legal challenge and renders evidence obtained lawful for all purposes.

4. Consequences of Not Following RIPA and IPA

4.1 Although not obtaining authorisation under RIPA does not make the authorisation unlawful, it does have consequences:

- evidence that is gathered may be inadmissible in court;
- the subjects of surveillance can bring their own claim on human rights grounds on the basis that the Council has infringed their rights under Article 8;
- if a challenge under Article 8 is successful, the Council would suffer reputational damage and may face a claim for financial compensation;
- the Government has also introduced a tribunal system to deal with complaints and any person who believes their rights have been breached can have their complaint dealt with by the Investigatory Powers Tribunal (IPT) (see section 59); and
- it is likely that the activity could be construed as an error and have to be investigated with a report submitted by the Council's SRO to the Investigatory Powers Commissioner's Office (IPCO) (see section 58).

4.2 If any Council officer obtains communications data without obtaining the appropriate authorisation through NAFN and OCDA, this is unlawful and is a criminal offence under IPA.

5. Independent Oversight

5.1 RIPA was originally overseen by the Office of Surveillance Commissioners (OSC). From 1 Sept 2017 oversight for both RIPA and IPA is now provided by the Investigatory Powers Commissioner's Office (IPCO). IPCO is the independent inspection office whose remit includes providing comprehensive oversight of the use of the powers to which RIPA, IPA and the Codes apply, and adherence to the practices and processes described therein. They also provide guidance to be followed which is separate to the Codes.

5.2 IPCO has unfettered access to all locations, documentation and information systems as is necessary to carry out its full functions and duties and will periodically inspect the records and procedures of the Council to ensure the appropriate authorisations have been given, reviewed, cancelled, and recorded properly.

5.3 It is the duty of any person who used investigatory powers to comply with any request made by a Commissioner to disclose or provide any information they require for the purpose of enabling them to carry out their functions. It is, therefore, important that the Council can show it complies with this Policy and with the provisions of RIPA and IPA.

PART B Surveillance Types and Criteria

6. Introduction

6.1 It is important to understand the definition of surveillance; what activities are classed as surveillance and the different types of surveillance covered by RIPA and the HRA. Surveillance can be both overt and covert and depending on their nature, are either allowed to be authorised under RIPA or not. There are also different degrees of authorisation depending on the circumstances.

7. Surveillance Definition

7.1 **Surveillance is:**

- 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, with or without the assistance of a device.

8. Overt Surveillance

8.1 Overt surveillance is where the subject of surveillance is aware that it is taking place, either by way of signage, e.g. in the use of CCTV or because the person who is the subject of the surveillance has been informed of the activity. Overt surveillance is outside the scope of RIPA and, therefore, does not require authorisation. However, it must still take account of privacy under the HRA and be necessary and proportionate. Any personal data obtained will also be subject to the DPA.

9. Covert Surveillance

9.1 Covert Surveillance is defined as “surveillance which is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place” and is covered by RIPA. Covert surveillance is categorised as either **intrusive** or **directed.**

9.2 There are three categories of covert surveillance regulated by RIPA:

(a) **Intrusive Surveillance** (the Council is **not** permitted to carry out intrusive surveillance)
(b) **Directed Surveillance**
(c) **Covert Human Intelligence Sources** (CHIS)

10. Intrusive Surveillance

10.1 The Council has no authority in law to carry out intrusive surveillance; only the Police and other law enforcement agencies can lawfully carry out this category of surveillance.

10.2 Intrusive surveillance is defined in section 26 (3) of the RIPA as covert surveillance that:

- is carried out in relation to anything taking place on any residential premises or in any private vehicle; and
- involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

10.3 Where surveillance is carried out in relation to anything taking place on any residential premises or in any private vehicle by means of a device, without that device being present on the premises, or in the vehicle, it is not intrusive unless the device consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle. Thus, an observation post outside premises, which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance.

10.4 A risk assessment of the capability of equipment being used for surveillance on residential premises and private vehicles, such as high-powered zoom lenses, should be carried out to ensure that its use does not meet the criteria of intrusive surveillance.

11. Directed Surveillance

11.1 The Council can lawfully carry out directed surveillance.

11.2 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); 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.

12. Private Information

12.1 The level of privacy that individuals can expect depends upon the nature of the environment they are in at the time, e.g. within an individual's own home or private vehicle, an individual can expect the highest level of privacy. The level of expectation of privacy may reduce if the individual transfers into public areas.

12.2 The relevant Codes provide guidance on what is private information. They state private information includes any information relating to a person's private or family life. As a result, private information is capable of including any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

12.3 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 although acting in public, and where a record is being made by the Council of that person's activities for future consideration or analysis. **Surveillance of publicly accessible areas of the internet should be treated in a similar way**, recognising that there may be an expectation of privacy over information which is on the internet, particularly when accessing information on social media websites. Prior to and during any internet or social media research, staff must take into account the privacy issues regarding any person associated with the research.

12.4 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information. In such circumstances, the totality of information gleaned may constitute private information even if individual records do not. Where such conduct includes covert surveillance, a directed surveillance authorisation may be considered appropriate.

12.5 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.

12.6 Information which is non-private may include publicly available information such as, books, newspapers, journals, TV and radio broadcasts, newswires, websites, mapping imagery, academic articles, conference proceedings, business reports, and more. Such information may also include commercially available data where a fee may be charged, and any data which is available on request or made available at a meeting to a member of the public.

12.7 An assessment must be made regarding the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance (see section 47).

13. Confidential or Privileged Material

13.1 Particular consideration needs to be given in cases where the subject of the investigation or operation might reasonably assume a high degree of confidentiality. This includes where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source, or where material contains confidential personal information or communications between a Member of Parliament and another person on constituency business. Directed surveillance likely or intended to result in the acquisition of knowledge of confidential or privileged material must be authorised by the Chief Executive.

13.2 Advice must be sought from the Council's Monitoring Officer if there is a likelihood of obtaining this type of material.

14. Lawful Grounds

14.1 The lawful grounds for directed surveillance is a higher threshold for the Council and cannot be granted unless it is to be carried out for the purpose of preventing or detecting criminal offence(s) which:

- meet the 'serious crime threshold', i.e. is punishable, whether on summary conviction or on indictment, 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 1933, i.e. relate to the sale of alcohol and tobacco to minors.

14.2 These are the only grounds available to the Council and hence the only justification.

14.3 Preventing or detecting crime goes beyond the prosecution of offenders and includes actions taken to avert, end or disrupt the commission of criminal offences.

15. Test Purchases

15.1 Test purchase activity does not in general require authorisation as a CHIS under RIPA as seller-purchaser activity does not normally constitute a relationship as the contact is likely to be limited. However, if a number of visits are undertaken at the same establishment to encourage familiarity, a relationship may be established and authorisation, as a CHIS, should be considered. If the test purchaser is wearing

recording equipment and is not authorised as a CHIS, or an adult is observing, consideration should be given to granting a directed surveillance authorisation if the surveillance meets the directed surveillance threshold, i.e. the covert surveillance is likely to obtain private information and the offence carries 6 months' imprisonment or involves the sale of alcohol or tobacco to children. If it does not meet the threshold, it is important that a full risk assessment is undertaken to ensure the HRA is properly

considered and it can be demonstrated that the activity is justified, i.e. necessary and proportionate.

15.2 Where test purchase activity does not meet the RIPA criteria/thresholds, the activity will be outside RIPA (non-RIPA) (see section 21), or where no private information is likely to be obtained, officers must consult with their line manager on the approach to be taken and a decision made on a case-by-case basis. Non-RIPA procedures should be followed where it is possible that private information may be obtained. For cases where no private information will be obtained, justification for undertaking test purchases should be recorded in relevant case file notes.

15.3 When conducting covert test purchase operations at more than one establishment, it is not necessary to construct an authorisation for each premises to be visited but the intelligence must be sufficient to prevent 'fishing trips'. Premises may be combined within a single authorisation providing that each premises is identified at the outset.

15.4 Necessity, proportionality and collateral intrusion must be carefully addressed in relation to each of the premises. It is unlikely that authorisations will be considered proportionate without demonstration that overt methods have been considered or attempted and failed (Section 245 OSC Procedures & Guidance 2016).

16. Urgent cases

16.1 There is no provision for the Council to authorise urgent oral authorisations under RIPA as all authorisations must be approved by a JP. If surveillance is required to be carried out in an urgent situation or as an immediate response, it must still be necessary and proportionate under HRA. This type of surveillance is surveillance outside of RIPA (non-RIPA) (see section 21). Officers must contact an AO, by telephone (or other appropriate means), to seek authorisation. The consequences of urgent surveillance action must be properly considered by the AO and the outcome(s) documented within relevant case file notes.

17. Surveillance for Preventing Disorder

17.1 Authorisation for the purpose of preventing disorder may only be granted if it involves criminal offence(s) punishable (whether on summary conviction or indictment) by a maximum term of at least 6 months' imprisonment. Surveillance for disorder not meeting these criteria would need to be carried out as surveillance outside of RIPA (non-RIPA) (see section 21).

18. Surveillance Camera Systems

18.1 Under Section 29 (6) of the Protection of Freedoms Act 2012, CCTV, along with other surveillance camera technology, is now referred to as 'surveillance camera systems' These systems include:

- closed circuit television (CCTV);
- body worn video (BWV);
- automatic number plate recognition (ANPR);

- deployable mobile overt mobile camera systems, e.g. deployed to detect waste offences such as fly-tipping;
- any systems for recording or viewing visual images for surveillance purposes;
- any systems for storing, receiving, transmitting, processing or checking images or information obtained by those systems; and
- any other systems associated with, or otherwise connected with those systems.

18.2 The 'surveillance camera systems' definition has far reaching implications as the use of any cameras that meet the requirement will have to be used in a manner that complies with the:

- Surveillance Camera Code of Practice 2013 (the 'surveillance camera systems' definition is repeated in this code);
- the Information Commissioner's Office (ICO) code, 'In the picture: a data protection code of practice for surveillance cameras and personal information'; and
- the DPA.

18.3 The use of conventional town centre CCTV systems operated by the Council do not normally fall under RIPA. However, it does fall under the DPA, the codes of practice referred to above and the Council's CCTV Policy. In addition, should there be a requirement for the CCTV cameras to be used for a specific purpose to conduct surveillance, it is likely that the activity will fall under directed surveillance and, therefore, require a RIPA authorisation.

18.4 Operators of the Council's CCTV system need to be aware of the implications of RIPA when using CCTV and that continued, prolonged and systematic surveillance of an individual may require a RIPA authorisation.

18.5 When the CCTV cameras are used in a directed surveillance situation, either by officers from relevant services within the Council or outside law enforcement agencies such as the Police, the Council's CCTV Policy should be followed as well as the RIPA Codes.

18.6 The CCTV staff must have a copy of the directed surveillance authorisation form in a redacted format, or a copy of the authorisation page. If it is an urgent oral authority from the Police, a copy of the applicant's notes must be retained or some other document, which confirms, in writing, the authorisation and exactly what has been authorised. It is important that CCTV staff check the authority and only carry out what is authorised. **A copy of the application or notes must be forwarded to the RIPA Coordinator to be recorded in the RIPA Central Register.** This will assist the Council to evaluate the authorisations and assist with oversight.

19. Automatic Number Plate Recognition (ANPR)

19.1 Automatic number plate recognition (ANPR) does not engage RIPA if it is used for the purpose it is registered for, such as traffic flow management or safety and enforcement within car parks. However, it is capable of being a surveillance device if used in a pre-planned way to carry out surveillance by monitoring a particular vehicle by plotting its locations, e.g. in connection with illegally depositing waste (fly-tipping).

19.2 Should it be necessary to use any ANPR systems to monitor vehicles, the same RIPA principles apply where a directed surveillance authorisation should be sought.

20. Internet and Social Media Investigations

20.1 The Council is a Public Authority in law under the HRA and, as such, staff must always adhere to this legislation. This applies when undertaking internet and social media investigations/research.

20.2 Researching, recording, storing, and using open source information regarding a person or group of people must be both necessary and proportionate and take account of the level of intrusion against any person. The activity may also require authorisation and approval by a Magistrate under RIPA. To ensure that any resultant interference with a person's Article 8 right to respect for their private and family life is lawful, the material must be retained and processed in accordance with the principles of the GDPR.

20.3 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources (i.e. internet and social media) available to the public, whether by payment or otherwise, which can be used as intelligence or evidence.

20.4 The use of online open source internet and social media research techniques has become a productive method of obtaining information to assist the Council with its regulatory and enforcement functions. It can also assist with service delivery issues and debt recovery. However, the use of the internet and social media is constantly evolving and with it the risks associated with these types of enquiries, particularly regarding breaches of privacy under Article 8 of the HRA and other operational risks.

20.5 The internet is another method of carrying out surveillance and a computer, which includes smartphones and tablets, are surveillance devices. Repeat viewing of individual open source sites for the purposes of intelligence gathering and data collation may constitute directed surveillance. Activities of monitoring through, for example, a social media profile over a period of time and a record of the information is kept for later analysis or evidential purposes is likely to require a RIPA authorisation. Where covert contact is made with another person on the internet a CHIS authority may be required.

20.6 Where activity is undertaken as described above, the RIPA application process and the contents of this Policy must be followed.

20.7 Where the activity falls within the criteria of surveillance or CHIS but is outside of RIPA, this will require authorising internally in accordance with non-RIPA procedures.

20.8 Any activity carried out over the internet leaves a trace or footprint, which can identify the device used and, in some circumstances, the individual carrying out the activity. This may pose a legal and reputational risk to the Council from a challenge by the subject of the research for breaching Article 8 of the HRA. There is also a risk of compromise to other investigations and, therefore, the activity must be conducted in a manner that does not compromise any current or future investigation or tactics.

20.9 To justify the research, there must be a clear lawful reason, and it must be necessary. The reason for the research, such as the criminal conduct that it is aimed to prevent or detect, must be identified and clearly described. This must be documented with clear objectives. Should the research fall within RIPA activity, the RIPA authorisation deals with this criterion for it to be lawful.

20.10 During the course of conducting internet open source research, the nature of the online activity may evolve. Staff must continually assess and review their activity to ensure it remains lawful and compliant. Where it evolves into RIPA activity, the RIPA procedure must be followed. If in doubt, staff must seek advice from their line manager and/or the RIPA Coordinator.

20.11 Any material gathered from the internet during the course of a criminal investigation must be retained in compliance with the CPIA Code of Practice and all material stored in line with the GDPR data retention policy.

20.12 There is restricted procedure guidance covering online open source research; this must be read and followed in conjunction with this Policy. Staff can gain access to this procedure through the RIPA Coordinator.

21. Surveillance Outside of RIPA

21.1 For directed surveillance under RIPA, the criminal offence under investigation must carry a minimum of a **6 months' imprisonment sentence** (directed surveillance serious crime threshold) or relate to the sale of alcohol or tobacco to children. This means that there are scenarios within an investigation that do not meet this threshold; nevertheless, surveillance may still be necessary for the purposes of the investigation. This surveillance will fall outside of RIPA ('non-RIPA') and includes surveillance relating to:

- anti-social behaviour disorder which does not attract a maximum custodial sentence of at least six months' imprisonment
- planning enforcement prior to the serving of a notice or to establish whether a notice has been breached
- most licensing breaches
- safeguarding vulnerable people
- civil matters
- disciplinary matters

21.2 The above scenarios are likely to be targeted surveillance, which may breach an individual's Article 8 rights to privacy and, therefore, the activity must be conducted in away that is HRA compliant, which will include consideration as to the necessity and proportionality of the surveillance activity.

21.3 To ensure that the above surveillance is undertaken in a manner that is compatible with HRA, officers must have due regard to the principles of RIPA, the Codes, and this Policy and, in practice, apply these as if the purposes for which the surveillance is being used fall within RIPA.

21.4 Non-RIPA surveillance also includes **surveillance for the purposes of disciplinary matters**. Guidance requires that this type of surveillance must be compliant with the

monitoring at work guidance that forms part of 'The employment practices code' issued by the ICO. This is to ensure this complies with the HRA.

21.5 Should a disciplinary investigation also involve a criminal offence which meets the RIPA criteria, e.g. including fraud, the option to carry out the surveillance under RIPA should be considered. However, it must be a genuine criminal investigation with a view to prosecuting the offender.

21.6 Should it be necessary to undertake surveillance for the purposes of disciplinary matters, advice must be sought from the Assistant Director for Workforce in conjunction with the RIPA Coordinator.

21.7 As part of the process of formally recording and monitoring surveillance that falls outside RIPA, 'non-RIPA' surveillance forms (application, review, renewal and cancellation) must be completed in the same manner as that for surveillance undertaken under RIPA and the surveillance authorised by an AO. In the first instance, this ought to be the AO for the Directorate to which the investigatory activity relates or, if they are not available, any of the designated AOs. A copy of non-RIPA surveillance forms can be obtained from the RIPA Coordinator.

21.8 All completed non-RIPA forms must be forwarded to the RIPA Coordinator who will maintain a central record of non-RIPA surveillance and ensure the SRO is informed of such activity. This will allow the SRO to maintain an oversight of non-RIPA surveillance to ensure it is compliant with the HRA and to prevent errors.

21.9 The following types of activity do **not** require RIPA authorisation:

- General observations that do not involve the systematic surveillance of an individual or a group of people and should an incident be witnessed the officer will overtly respond to the situation
- Use of overt CCTV and ANPR systems
- Surveillance where no private information is likely to be obtained
- Surveillance undertaken as an immediate response to a situation
- Covert surveillance not relating to a criminal offence which carries a maximum sentence of 6 months' imprisonment or relate to the sale of alcohol or tobacco to children (this is likely to be surveillance outside of RIPA)
- The use of a recording device by a CHIS in respect of whom an appropriate use or conduct authorisation has been granted permitting them to record any information in their presence
- The covert recording of noise where the recording is of decibels only or constitutes non-verbal noise (such as music, machinery or an alarm), or the recording of verbal content is made at a level which does not exceed that which can be heard from the street outside or adjoining property with the naked ear; in the latter circumstance, the perpetrator would normally be regarded as having forfeited any claim to privacy (in either circumstance this is outside of RIPA)

22. Joint Agency Surveillance

22.1 In cases where one agency is acting on behalf of another, it is usually for the tasking agency to obtain or provide the authorisation. For example, where surveillance is carried out by Council employees on behalf of the Police, authorisation would be sought by the Police. If it is a joint operation involving both agencies, the lead agency should seek authorisation.

22.2 Council staff involved with joint agency surveillance are to ensure that all parties taking part are authorised on the authorisation form to carry out the activity. When staff are operating on another organisation's authorisation, they are to ensure they see what activity they are authorised to carry out and make a written record. They must also provide a copy of the authorisation to the RIPA Coordinator. This will assist with oversight of the use of Council staff carrying out these types of operations. Line Managers must be made aware if their staff are involved in this type of surveillance.

23. Use of Third-Party Surveillance

23.1 In some circumstances it may be appropriate or necessary for the Council to work with third parties who are not themselves a Public Authority (such as an individual, company or non-governmental organisation) to assist with an investigation. Where that third party is acting in partnership with or under the direction of the Council, then they are acting as our agent and any activities that the third-party conducts, which meet the RIPA definitions of directed surveillance must be authorised. This is because the agent will be subject to RIPA in the same way as any employee of the Council. The AO must ensure that the agents are qualified or have the necessary skills to achieve the objectives. They must also ensure that they understand their obligations under RIPA. If advice is required, contact the RIPA Coordinator.

23.2 Similarly, a surveillance authorisation must also be considered where the Council is aware that a third party (that is not a Public Authority), e.g. activist groups/individuals, RSPCA, Federation Against Copyright Theft (FACT), is independently conducting surveillance and the Council intends to make use of any suitable material obtained by the third party for the purposes of a specific investigation.

24. Surveillance Equipment

24.1 The Council will maintain a central register of all surveillance equipment, including all types of camera and noise monitoring devices. This will require a description, serial number, and an explanation as to the equipment's capabilities. It is recognised that smartphones are surveillance devices; however, they will not be recorded on the central register as officers should not ordinarily use such devices to undertake surveillance due to the associated evidential risks.

24.2 The register will be held and maintained by the RIPA Coordinator or a designated deputy. This equipment is available for all service areas to deploy.

24.3 All equipment capable of being used for directed surveillance must be fit for the purpose for which it is intended.

24.4 When completing an authorisation (where under RIPA or outside RIPA), the applicant must provide the AO with details of any equipment to be used and its technical capabilities. The AO will have to take this into account when considering the intrusion issues, proportionality and whether the equipment is fit for the required purpose. The AO must make it clear on the authorisation exactly what equipment, if any, they are authorising and in what circumstances it will be deployed.

24.5 All surveillance equipment must be stored securely to prevent unauthorised use. A log must be created and maintained to record the date/time the equipment was removed from storage, by whom, for what purpose and the date/time it was returned to storage and by whom.

PART C Covert Human Intelligence Sources (CHIS)

25. Introduction

25.1 RIPA covers the activities of Covert Human Intelligence Sources (CHIS) which relates not only to sources commonly known as informants (members of the public providing the Council with information), but also the activities of undercover officers. It matters not whether they are employees of the Council, agents or members of the public engaged by the Council to establish or maintain a covert relationship with someone to obtain information.

25.2 Not all human source activity will meet the definition of a CHIS; for example, a source may be a public volunteer or someone who discloses information out of professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship. However, officers must be aware that such information may have been obtained in the course of an ongoing relationship with a family member, friend or business associate. The Council has a duty of care to all members of the public who provide information to us and appropriate measures must be taken to protect that source. How the information was obtained should be established to determine the best course of action. The source and information should also be managed correctly in line with CPIA and the disclosure provisions.

25.3 Recognising when a source becomes a CHIS is important as this type of activity may need authorisation. Should a CHIS authorisation be required, all of the staff involved in the process must make themselves fully aware of the contents of this Policy and the CHIS Code.

25.4 A CHIS, their conduct, and the use to which they are put is defined within Section 26 (7) and (8) of RIPA. Chapter 2 of the relevant Code provides examples of where this regime may apply.

26. Definition of a CHIS

26.1 Individuals act as a CHIS if they:

- establish or maintain a covert relationship with another person to obtain information;
- covertly give access to information to another person; or
- disclose information covertly which they have obtained using the relationship or they have obtained because the relationship exists.

26.2 A relationship is established, maintained or used for a covert purpose if, and only if, it is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. The relationship between the Council officer and the person providing the information is not covert. It relates to how the information was either obtained or will be obtained, i.e. was it or will it be obtained from a third party without them knowing it was being passed on to the Council? This would amount to a covert relationship.

26.3 It is possible that a person will become engaged in the conduct of a CHIS without the Council inducing, asking or assisting the person to engage in that conduct. An authorisation must be considered, for example, where the Council is aware that a third party is independently maintaining a relationship, i.e. 'self-tasking', in order to obtain evidence of criminal activity, and the Council intends to make use of that material for its own investigative purposes.

27. Vulnerable and Juvenile CHIS

27.1 Special consideration must be given to the use of a 'Vulnerable Individual' as a CHIS. A 'Vulnerable Individual' is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of him/herself, or unable to protect him/herself against significant harm or exploitation. Any individual of this description, or a 'Juvenile' as defined below, should only be authorised to act as a source in the most exceptional circumstances and only then when authorised by the Chief Executive or, in his absence, the officer acting as the Deputy Chief Executive.

27.2 Special safeguards also apply to the use or conduct of Juvenile Sources; that is sources under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against their parents or any person who has parental responsibility for them.

27.3 If the use of a Vulnerable Individual or a Juvenile is being considered as a CHIS you must consult the Council's Monitoring Officer before authorisation is sought.

27.4 Authorisations should not be granted in respect of a Juvenile CHIS unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000 (SI No. 2793) are satisfied.

28. Lawful Grounds

28.1 The lawful grounds for a CHIS authorisation is prevention and detection of crime and prevention of disorder. The serious crime threshold in relation to the offence under consideration carrying a minimum of 6-months' imprisonment sentence does not apply to a CHIS.

28.2 Authorisations for Juvenile Sources must be authorised by the Chief Executive or, in their absence, the officer undertaking the role of the Deputy Chief Executive.

29. Conduct and Use of a Source

29.1 The way the Council uses a CHIS for covert activities is known as 'the use and conduct' of a source.

29.2 The use of a CHIS involves any action on behalf of the Council to induce, ask or assist a person to engage in the conduct of a CHIS, or to obtain information by means of the conduct of a CHIS.

29.3 The conduct of a CHIS is establishing or maintaining a personal or other relationship with another person for the covert purpose of:

(a) using such a relationship to obtain information, or to provide access to information to another person; or
(b) disclosing information obtained by the use of such a relationship or as a consequence of such a relationship; or
(c) is incidental to anything falling within (a) and (b) above.

29.4 In other words, an authorisation for conduct will authorise steps taken by the CHIS on behalf, or at the request, of the Council.

29.5 The use of a source is what the Council does in connection with the source, such as tasking (see section 32), and the conduct is what a source does to fulfil whatever tasks are given to them or which is incidental to it. The use and conduct require separate consideration before authorisation; however, they are normally authorised within the same authorisation.

29.6 The same authorisation form is used for both use and conduct. A 'Handler' and 'Controller' must be designated as part of the authorisation process and the application can only be authorised if necessary and proportionate. Detailed records of the use, conduct and tasking of the source must be maintained (see section 36).

29.7 Care must be taken to ensure that the CHIS is clear on what is or is not authorised at any given time, and that all the CHIS activity is properly risk assessed, and that relevant applications, reviews, renewals and cancellations are correctly performed.

29.8 Careful consideration must be given to any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration must also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS.

30. Handler and Controller

30.1 CHIS may only be authorised if the following arrangements are in place:

- That there will at all times be an officer, the **Handler**, within the Council who will have day to day responsibility for dealing with the source on behalf of the authority, and for the source's security. The Handler is likely to be the investigating officer.
- That there will at all times be another officer within the Council who will have general oversight of the use made of the source, the **Controller**. This is likely to be the Handler's line manager.
- That there will at all times be an officer within the Council who has responsibility for maintaining a record of the use made of the source; see CHIS record keeping (see section 36).

30.2 The **Handler** will have day to day responsibility for:

- dealing with the source on behalf of the Council;
- risk assessments;
- directing the day-to-day activities of the source;
- recording the information supplied by the source;
- monitoring the source's security and welfare; and
- informing the Controller of concerns about the personal circumstances of the CHIS that might affect the validity of the risk assessment or conduct of the CHIS.

30.3 The **Controller** will be responsible for:

- the management and supervision of the Handler;
- general oversight of the use of the CHIS; and
- maintaining an audit of case work sufficient to ensure that the use or conduct of the CHIS remains within the parameters of the extant authorisation.

31. Undercover Officers

31.1 Oversight and management arrangements for **undercover operatives**, while following the principles of RIPA, will differ, in order to reflect the specific role of such individuals when they are officers of the Council. The role of the Handler will be undertaken by a person referred to as a **'Cover Officer'**. The Cover Officer will be required to ensure the welfare of Council undercover operatives, including where the undercover work is being undertaken online.

32. Tasking

32.1 Tasking is the assignment given to the source by the Handler or Controller, e.g. asking them to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the Council. Authorisation for the use or conduct of a source is required prior to any tasking where such tasking requires the source to establish or maintain a personal or other relationship for a covert purpose.

32.2 In some instances, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose, e.g. a member of the public is asked to maintain a record of all vehicles arriving and leaving a specific location or to record the details of visitors to a neighbouring house. A relationship has not been established or maintained in order to gather the information and a CHIS authorisation is, therefore, not available or required. Other authorisations under RIPA, e.g. directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

32.3 CHIS authorisations should not be drawn so narrowly that a separate authorisation is required each time the CHIS is tasked; rather, an authorisation might cover, in broad terms, the nature of the source's task.

33. Risk Assessments

33.1 The Council has a responsibility for the safety and welfare of the source and for the consequences to others of any tasks given to the source. It is a requirement of the Code that a risk assessment is carried out. This must be submitted with the authorisation request. The risk assessment must provide details of how the CHIS is going to be handled. It must take into account the safety and welfare of the CHIS in relation to the activity and must consider the likely consequences should the role of the CHIS become known. The ongoing security and welfare of the CHIS after the cancellation of the authorisation must also be considered at the outset.

34. Use of Equipment by a CHIS

34.1 If a CHIS is required to wear or carry a surveillance device, such as a covert camera, it does not require a separate intrusive or directed surveillance authorisation providing the device will only be used in the presence of the CHIS. It should be authorised as part of the conduct of the CHIS.

34.2 CHIS, whether or not wearing or carrying a surveillance device, in residential premises or a private vehicle, does not require additional authorisation to record any activity taking place inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations; however, this must be identified at the planning stage.

34.3 Councils cannot authorise intrusive directed surveillance, e.g. accessing private homes or vehicles to conceal surveillance equipment for the purposes of monitoring. However, this does not prevent intrusive CHIS activity, e.g. authorisation of an undercover Council officer for the purposes of purchasing illicit tobacco, which leads to the officer entering a private home to collect a previously agreed purchase of the tobacco.

35. CHIS Management

35.1 The operation will require managing by the Handler and Controller, which will include ensuring that the activities of the source and the operation remain focused and there is

no status drift. It is important that the intrusion is assessed to ensure the operation remains proportionate. The security and welfare of the source will also be monitored. The AO must maintain general oversight of these functions.

35.2 During CHIS activity, there may be occasions when unforeseen actions or undertakings occur. Such incidences must be recorded as soon as practicable after the event and if the existing authorisation is insufficient it must either be dealt with by way of a review and re-authorised (minor amendments only) or it must be cancelled and a new authorisation obtained before any further action is carried out.

35.2 Similarly, where it is intended to task a CHIS in a new significantly different way than previously identified, the proposed tasking must be referred to the AO who must consider whether a separate authorisation is required. This must be done in advance of any tasking and details of such referrals must be recorded.

36. CHIS Record Keeping

36.1 Centrally Retrievable Record of Authorisations

36.2 A centrally retrievable record of all authorisations is held by the Council. This record contains the relevant information to comply with the Codes. These records are updated whenever an authorisation is granted, renewed or cancelled and are available to IPCO upon request.

36.3 The records are retained for 5 years from the ending of the authorisation.

36.4 Individual Source Records of Authorisation and Use of CHIS

36.5 Detailed records must be kept of the authorisation and the use made of a CHIS. An AO must not grant an authorisation for the use or conduct of a CHIS unless they believe that there are arrangements in place for ensuring that there is, at all times, a person with the

responsibility for maintaining a record of the use made of the CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000 (SI No: 2725) details the particulars that must be included in these records.

36.6 The particulars to be contained within the records are:

a. identity of the source;
b. identity, where known, used by the source;
c. any relevant investigating authority other than the authority maintaining the records;
d. the means by which the source is referred to within each relevant investigating authority;
e. any other significant information connected with the security and welfare of the source;
f. any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in paragraph (d) has been

g. 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;
h. the date when and the circumstances in which the source was recruited;
i. identity of the Handler and Controller (and details of any changes);
j. the periods during which those persons have discharged those responsibilities;
k. the tasks given to the source and the demands made of him in relation to his activities as a source;
l. all contacts or communications between the source and a person acting on behalf of any relevant investigating authority;
m. the information obtained by each relevant investigating authority by the conduct or use of the source;
n. any dissemination by that authority of information obtained in that way; and
o. in the case of a source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority.

36.7 The RIPA Coordinator shall maintain these records.

36.8 Council officers shall maintain auditable records for individuals or members of organisations (e.g. travel agents, housing associations and taxi/private hire companies) that may provide intelligence but who do not meet the definition of a CHIS. This will include **repeat supply of information** where an individual is obtaining the information through a covert relationship. This will assist the Council to monitor the status of a human source and identify whether that person should be duly authorised as a CHIS. This should be updated regularly to explain why authorisation is not considered necessary. This responsibility rests with the designated AOs within the Council.

36.9 In some cases, individuals provide information but do not wish to be registered as a CHIS or they repeatedly provide information that has not been sought or the Council does not wish to authorise the individual as a CHIS, e.g. because there is evidence of

unreliability. If the information being provided is recorded as potentially useful or actionable, there is a potential duty of care to the individual and this means the designated AOs must manage the individual properly.

36.10 The AOs must ensure sensible and verifiable procedures are in place to monitor for ‘status drift’ and where it becomes clear that the individual meets the definition of a CHIS, the AO must take steps to either ensure the activity ceases or a decision is made to grant a CHIS authorisation. Where an authorisation is granted the AO must take account of the difference between a volunteer of information already known to the individual and the relevance of the exploitation of a relationship for a covert purpose.

36.11 Further Documentation

36.12 In addition to the above, when appropriate, records or copies of the following are retained by the Council for 5 years:

a. a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
b. a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
c. the reason why the person renewing an authorisation considered it necessary to do so;
d. any risk assessment made in relation to the CHIS;
e. the circumstances in which tasks were given to the CHIS;
f. the value of the CHIS to the investigating authority;
g. a record of the results of any reviews of the authorisation;
h. the reasons, if any, for not renewing an authorisation;
i. the reasons for cancelling an authorisation;
j. the date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease; and
k. a copy of the decision by a Judicial Commissioner on the renewal of an authorisation beyond 12 months (where applicable).

36.13 The RIPA Coordinator shall maintain these records.

36.14 The records kept by the Council must be maintained in such a way as to preserve the confidentiality, or prevent disclosure of the identity of the CHIS, and the information provided by that CHIS.

36.15 Combined Authorisations

36.16 Where investigatory activity is likely to involve both the use of a CHIS and directed surveillance, RIPA practice permits the two types of authorisations to be legally combined onto one application. However, it is the Council's practice for separate forms to be completed to maintain the distinction between the two techniques being used.

PART D RIPA Roles and Responsibilities

37. Council Members

37.1 Cabinet shall set and/or agree continuance of this Policy, as appropriate.

38. Audit Committee

38.1 The use of RIPA, IPA and non-RIPA by Council officers shall be reported to the Audit Committee on a regular basis. Where the Audit Committee is satisfied that RIPA, IPA

and non-RIPA practices are being used consistently within the Policy and that the Policy remains fit for purpose then the Policy may continue to operate without wider consideration or revision by Cabinet.

38.2 Where there are any concerns about the manner in which RIPA, IPA and non-RIPA practices are being used or that the policy is not fit for purpose, the Audit Committee may direct that these concerns are reported to Cabinet or, if necessary, to full Council and require the SRO to oversee a review and revision of the Policy to ensure it is fit for purpose.

39. Senior Responsible Officer

39.1 The nominated SRO is the Executive Director of People. The SRO has responsibilities for:

- the integrity of the processes in place within the Council to authorise directed surveillance and CHIS;
- compliance with the relevant sections of RIPA and the Codes;
- oversight of the reporting of errors to IPCO and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- engagement with IPCO and the inspectors who support the Commissioner when they conduct their inspections;
- where necessary, overseeing the implementation of any recommended post-inspection action plans;
- ensuring that all AOs are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner;
- ensuring that officers who verify communications data applications are of an appropriate seniority within the Council and informing NAFN of such nominations; and
- being aware of any applications for communications data being made before they are submitted to OCDA

40. RIPA Coordinator

40.1 The RIPA Coordinator is the Head of Business and Consumer Protection and is responsible for storing all original authorisations, reviews, renewals and cancellation forms and the signed approval or refusal documentation from the JP. This will include any authorisations that have not been authorised by an AO or refused by a JP.

40.2 The RIPA Coordinator will:

- keep the copies of the forms for a period of at least 5 years;
- keep the Central Register of all the authorisations, renewals and cancellations and issue the unique reference number;
  keep a database for identifying and monitoring expiry dates and renewal dates;

- along with the Executive and Assistant Directors, Service Managers, AOs, and Investigating Officers, ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Councils information management policies, departmental retention schedules and the DPA;
- provide administrative support and guidance on the processes involved;
- monitor the authorisations, renewals and cancellations with a view to ensuring consistency throughout the Council;
- monitor each service's compliance and act on any cases of non-compliance;
- signpost to further guidance and awareness of RIPA and the provisions of this Policy;
- arrange for the provision of training; and
- review the contents of this Policy.

41. Line Manager Responsibility and Management of the Activity

41.1 Line Managers within each service of the Council are responsible for ensuring that in all cases where surveillance is required, due consideration is given to the need for covert surveillance before an application is made for authorisation. This includes the consideration of using overt action, routine enquiries or inspections, which are less intrusive. Where it is considered that such less intrusive actions are not appropriate, Line Mangers must ensure that the rationale for this is fully understood and justified.

41.2 If authorised, it is important that all those involved in undertaking directed surveillance activities, including Line Managers, are fully aware of the extent and limits of the authorisation. There must be an ongoing assessment for the need for the activity to continue including ongoing assessments of the intrusion. All material obtained, including evidence, must be stored in line with relevant legislation and procedures to safeguard its integrity and reduce a risk of challenge (see section 53).

41.3 Line Managers must also ensure that the relevant reviews, renewals and cancellations (see **Appendix C**) are completed by the applicant in accordance with the Codes and the dates set throughout the process.

42. Investigating Officers/Applicant

42.1 The applicant is normally an Investigating Officer who completes the application section of the RIPA form. Investigating Officers must think about the need to undertake directed surveillance or the use of a CHIS before they seek authorisation and discuss it with their Line Manager. Investigating Officers must consider whether they can obtain the information or achieve their objective by using techniques other than covert surveillance.

42.2 The applicant or another appropriate person must carry out a feasibility study and this must be seen by the AO prior to or as part of the application. The feasibility study aims to ensure that the surveillance operation is practically possible, that risks are minimised and limiting factors that may impede the success of the operation are managed. The person seeking the authorisation must then complete the application form having regard to the guidance given in this Policy and the statutory Codes. There must not be any significant delay between the feasibility study and the completion of the application form

to ensure that the details within the application are accurate and will not have changed. The form must then be submitted to the AO for authorisation.

42.3 The applicant is expected to attend court to seek the approval of a JP and, if approved, and involved in the covert activity they must only carry out what is authorised and approved. They, or another appropriate person, will also be responsible for the submission of any reviews, renewals and cancellations.

43. Authorising Officer

43.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for the Council the AO must be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation.

43.2 The designated AOs within the Council who can grant authorisations are listed in **Appendix B**. They are all at Service Manager level or above. The AOs are also designated as being sufficiently senior within the Council for the purposes of verifying applications for communications data.

43.3 The role of the AO is to consider whether to authorise, review, or renew an authorisation. They must consider the facts of each investigation or operation involving surveillance individually on its own merits. They must also officially cancel the RIPA covert activity.

43.4 AOs must have been trained to an appropriate level so as to understand the requirements in the Codes and this training must be satisfied before an application is authorised.

43.5 AOs must not ordinarily be responsible for authorising investigations or operations in which they are directly involved. Where this occurs, the AO must record the rationale/justification for this and the central record of authorisations must highlight it, and it must be brought to the attention of a Commissioner or Inspector during their next inspection.

44.6 Authorisations must be given in writing by the AO by completing the relevant section on the authorisation form. When completing an authorisation, the case must be presented in a fair and balanced way; in particular, all reasonable efforts must be made to take into account information that weakens the case for the authorisation.

44.7 Obtaining an authorisation under RIPA will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. AOs must, therefore, explain why they believe the activity is both necessary (see section 45) and proportionate (see section 46) to what it seeks to achieve. AOs must also consider any similar activity which may be taking place, or sensitivities in the area.

44.8 Where there is any indication that an application for an authorisation may target or relate to individuals already known to social services (particularly in relation to individuals with learning disabilities and/or behaviour that is impacted by mental health) or where there is reasonable belief that individuals may be eligible for such services, the AO responsible for determining the application must take advice from the appropriate social care

Assistant Director or Service Manager to inform their decision as to whether the surveillance will be necessary and/or proportionate and to determine if there are any alternative courses of action that are more appropriate.

44.9 If AOs do not believe that the surveillance is necessary and proportionate to what it seeks to achieve **or** if other less intrusive methods may be used to obtain the information **or** insufficient steps are in place to reduce collateral intrusion, AOs must not grant authorisation.

44.10 If an AO considers authorisation may be granted, they also need to explain exactly what they are authorising, against whom, in what circumstances, where, over what period, etc. and that the level of the surveillance is appropriate to achieve the objectives. It is important that this is made clear on the authorisation as the surveillance operatives are only allowed to carry out what is authorised. This will assist with avoiding errors.

44.11 If any equipment, such as covert cameras are to be used, the AO needs to know the capability of the equipment before authorising its use. This will have an impact on collateral intrusion, necessity and proportionality. They must not rubber-stamp a request. It is important that they consider all the facts to justify their decision.

44.12 The AO may be required to attend court to justify what they authorised both as part of the judicial approval process or in any subsequent court trials or other tribunals.

44.13 AOs must acquaint themselves with the relevant Codes issued by the Home Office regarding RIPA and IPA. The must also be aware of the current Procedures and Guidance issued by IPCO (or previously by OSC); this document details operational guidance that must be followed. It is recommended that AOs hold their own copy of this document. This can be obtained from the RIPA Coordinator.

45. Necessity

45.1 RIPA and IPA first requires that the person granting an authorisation believes that the authorisation is **necessary** in the circumstances of the particular case for one or more of the statutory grounds (see section 14).

45.2 The applicant and AO must also be able to demonstrate why it is necessary to carry out the covert activity to achieve the objectives and that there are no other means of obtaining the same information in a less intrusive method. This is a specific part of the authorisation form.

46. Proportionality

46.1 If the activities are deemed necessary, the AO must also believe that they are **proportionate** to what is sought to be achieved by carrying them out. This involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms. What is the benefit of carrying out the activity, including any internet or social media research/investigation? How will the benefit outweigh the intrusion?

46.2 The authorisation/activity will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised is expected to bring a benefit to the investigation or operation and must not be disproportionate or arbitrary. The fact that a suspected offence may be serious will not of itself render the proposed actions proportionate. Similarly, an offence may be so minor that any deployment of covert techniques would be disproportionate. No activity will be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means. All activity much be carefully managed to meet the objective in question and must not be arbitrary or unfair.

46.3 When explaining proportionality, the AO must explain why the methods and tactics to be adopted during the surveillance is not disproportionate.

46.4 The Codes provide guidance relating to proportionality which must be considered by both applicants and AOs. These include:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;
- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;
- considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the necessary result; and
- evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

47. Collateral Intrusion

47.1 Before authorising applications for directed surveillance, the AO must also take into account the risk of obtaining **collateral intrusion**, which is private information about persons who are not subjects of the surveillance.

47.2 Staff must take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance. Where such collateral intrusion is unavoidable, the activities may still be authorised, providing this intrusion is considered proportionate to what is sought to be achieved. The same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

47.3 All applications must include an assessment of the risk of collateral intrusion and detail the measures taken to limit this to enable the AO to fully consider the proportionality of the proposed actions. This is detailed in a specific section within the authorisation form.

47.4 In order to give proper consideration to collateral intrusion, an AO must be given full information regarding the potential scope of the anticipated surveillance, including the likelihood that any equipment deployed may cause intrusion on persons or property other than the subject(s) of the application. If an automated system, such as an online search engine, is used to obtain the information, the AO must be made aware of its potential extent and limitations.

47.5 Material which is not necessary or proportionate to the aims of the operation or investigation must be discarded or, where it may be required for future evidential purposes, securely retained separately. It may also need retaining under CPIA. The AO must ensure appropriate safeguards for the handling, retention or destruction of such material, as well as compliance with DPA requirements.

47.6 Where it is proposed to conduct surveillance activity specifically against individuals who are not suspected of direct or culpable involvement in the overall matter being investigated, interference with the privacy of such individuals must not be considered as collateral intrusion but rather as intended intrusion.

47.7 In the event that authorised surveillance unexpectedly and unintentionally interferes with the privacy of any individual other than the intended subject, the AO must be informed by the applicant or the Investigating Officer by submitting a review form. Consideration must be given in any such case as to the need for any separate or additional authorisation.

47.8 Where the Council intends to access a social media or other online account to which they have been given access with the consent of the owner, the Council will still need to consider whether the account(s) may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation must be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

Part E Central Record and Safeguarding the Material

48. Introduction

48.1 AOs, applicants and Line Managers of relevant services may keep whatever records they deem appropriate to administer and manage the RIPA application process. This includes for the purpose of any legal obligations under the CPIA. However, this will not replace the requirements under the Codes, which includes the fact that the Council must hold a centrally held and retrievable record.

49. Central Record

49.1 The centrally retrievable record of all authorisations shall be held and maintained by the RIPA Coordinator. It will be regularly updated whenever an authorisation is applied for, refused, granted, renewed or cancelled. The record will be made available to the relevant Commissioner or an Inspector from IPCO, upon request.

49.2 It is the responsibility of the AOs to ensure all original authorisations and copies of Judicial applications/order forms, whether authorised or refused, together with review, renewal and cancellation documents, are sent to the RIPA Coordinator, within 5 working days, for inclusion in the central record of authorisations. The RIPA Coordinator will

ensure that all records are held securely with no unauthorised access. If in paper format, they must be forwarded in a sealed envelope marked **CONFIDENTIAL**.

49.3 The documents contained in the centrally held register must be retained for five years from the ending of the authorisation and destroyed in accordance with the period stipulated by the Council's document retention policy.

49.4 The centrally held register contains the following information:

- if refused, (the application was not authorised by the AO) a brief explanation of the reason why and the refused application should be retained as part of the central record of authorisation;
- if granted, the type of authorisation and the date the authorisation was given;
- details of attendances at the Magistrates' Court to include the date of attendances at court, the determining magistrate, the decision of the court and the time and date of that decision;
- name and rank/grade of the AO;
- the unique reference number (URN) of the investigation or operation;
- the title of the investigation or operation, including a brief description and names of subjects, if known;
- frequency and the result of each review of the authorisation;
- if the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date renewed by the JP;

- whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice;
- the date the authorisation was cancelled;
- authorisations by an AO where they are directly involved in the investigation or operation and if this has taken place it must be brought to the attention of a Commissioner or Inspector during their next RIPA inspection.

49.5 As well as the central record, the RIPA Coordinator shall also retain:

- the original of each application, review, renewal and cancellation, copy of the judicial application/order form, together with any supplementary documentation of the approval given by the AO;
- the frequency and result of reviews prescribed by the AO;
- the date and time when any instruction to cease surveillance was given;
- the date and time when any other instruction was given by the AO;
- a record of the period over which the surveillance has taken place, and this should have been included within the cancellation form.

49.6 These documents must also be retained for five years from the ending of the authorisation.

50. Safeguarding and the Use of Surveillance Material

50.1 This section provides guidance on the procedures and safeguards to be applied in relation to the handling of any material obtained through directed surveillance or CHIS activity. This material may include private, confidential or legal privilege information. It will also show the link to other relevant legislation.

50.2 The Council must ensure that their actions when handling information obtained by means of covert surveillance or CHIS activity comply with relevant legal frameworks and the Codes, so that any interference with privacy is justified in accordance with Article 8 (2) of the ECHR. Compliance with these legal frameworks, including data protection requirements, will ensure that the handling of private information obtained continues to be lawful, justified and strictly controlled, and is subject to robust and effective safeguards. The material will also be subject to the CPIA.

51. Authorised Purpose

51.1 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes. For the purposes of the RIPA Codes, something is necessary for the authorised purposes if the material:

- is, or is likely to become, necessary for any of the statutory purposes set out in RIPA in relation to covert surveillance or CHIS activity;
- is necessary for facilitating the carrying out of the functions of public authorities under RIPA;

- is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- is necessary for the purposes of legal proceedings; or
- is necessary for the performance of the functions of any person by or under any enactment.

52. Handling and Retention of Material

52.1 All material associated and obtained with an application will be subject to the provisions of the DPA and CPIA Codes of Practice. All officers involved within this process must make themselves aware of the provisions within this legislation and how it impacts on the whole RIPA process. Material obtained, together with relevant associated paperwork, must be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

52.2 Material required to be retained under CPIA must be retained until a decision is taken whether to institute proceedings against a person for an offence or if proceedings have been instituted, at least until the accused is acquitted or convicted or the prosecutor decides not to proceed with the case.

52.3 Where the accused is convicted, all material which may be relevant must be retained at least until the convicted person is released from custody, or six months from the date of conviction, in all other cases.

52.4 If the court imposes a custodial sentence and the convicted person is released from custody earlier than six months from the date of conviction, all material which may be relevant must be retained at least until six months from the date of conviction.

52.5 If an appeal against conviction is in progress when released, or at the end of the period of six months, all material which may be relevant must be retained until the appeal is determined.

52.6 If retention is beyond these periods, it must be justified under DPA. Where a service has undertaken surveillance, they must ensure that the material associated and obtained as a result of the surveillance is reviewed, retained and destroyed in accordance with the Council's and service's data retention schedules to ensure that the data is retained lawfully and only for as long as is necessary.

53. Use of Material as Evidence

53.1 Material obtained through directed surveillance, may be used as evidence in criminal proceedings. The admissibility of evidence is governed primarily by the common law, the CPIA, the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1996 and the HRA.

53.2 Ensuring the continuity and integrity of evidence is critical to every prosecution. Accordingly, considerations as to evidential integrity are an important part of the disclosure regime under the CPIA and these considerations will apply to any material acquired through covert surveillance that is used in evidence. When information obtained under a covert surveillance authorisation is used evidentially, the Council must be able to demonstrate how the evidence has been obtained, to the extent required by the relevant rules of evidence and disclosure.

53.3 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it must be retained in accordance with established disclosure requirements. In a criminal case the codes issued under CPIA will apply. They require that the investigator record and retain all relevant material obtained in an investigation and later disclose relevant material to the Prosecuting Solicitor. They in turn will decide what is disclosed to the Defence Solicitors.

53.4 There is nothing in RIPA that prevents material obtained under directed surveillance authorisations from being used to further other investigations

54. Dissemination of Information

54.1 It may be necessary to disseminate material acquired through the RIPA covert activity within the Council or to share it outside with other Councils or agencies, including the Police. The number of persons to whom any of the information is disclosed, and the extent of disclosure, must be limited to the minimum necessary. It must also be in

connection with an authorised purpose (see section 51). It will be necessary to consider exactly what and how much information should be disclosed. Only as much of the material may be disclosed as the recipient needs, e.g. if a summary of the material will suffice, no more than that should be disclosed.

54.2 The obligations apply not only to the Council, as the original authority acquiring the information, but also to anyone to whom the material is subsequently disclosed. In some cases, this will be achieved by requiring the latter to obtain permission from the Council before disclosing the material further. It is important that the Officer in Charge (OIC) of the enquiry considers these implications at the point of dissemination to ensure that safeguards are applied to the data.

54.3 A record must be maintained justifying any dissemination of material. If in doubt, seek advice from the RIPA Coordinator.

55. Storage

55.1 Material obtained through covert surveillance and CHIS authorisations, and all copies, extracts and summaries of it, must be handled and stored securely, so as to minimise the risk of loss. It must be held so as to be inaccessible to persons who are not required to see the material. This requirement to store such material securely applies to all those who are responsible for the handling of the material. It will be necessary to ensure that both physical and IT security and an appropriate security clearance regime is in place to safeguard the material.

56. Copying

56.1 Material obtained through covert surveillance may only be copied to the extent necessary for the authorised purposes set out above. Copies include not only direct copies of the whole of the material, but also extracts and summaries which identify themselves as the product of covert surveillance, and any record which refers to the covert surveillance and the identities of the persons to whom the material relates.

57.2 In the course of an investigation, the Council must not act on or further disseminate legally privileged items unless it has first informed the Investigatory Powers Commissioner that the items have been obtained.

57. Destruction

57.1 Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, must be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out above. If such information is retained, it must be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the data impossible.

Part F Errors and Complaints

58. Errors

58.1 Errors can have very significant consequences on an affected individual's rights. Proper application of the surveillance and CHIS provisions in the RIPA Codes and this Policy should reduce the scope for making errors.

58.2 It is important that all staff involved in the RIPA process report any issues, so they can be assessed as to whether it constitutes an error which requires reporting.

58.3. There are two types of errors within the Codes which are:

- relevant error
- serious error

58.4 Relevant Error

58.5 An error must be reported if it is a '**relevant error**'. A relevant error is any error by the Council in complying with any requirements that are imposed on it by any enactment which are subject to review by a Judicial Commissioner. This includes compliance by the Council with RIPA and the content of the Codes.

58.6 Examples of relevant errors occurring would include circumstances where:

- Surveillance activity has taken place without lawful authorisation
- There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes relating to the safeguards of the material

58.7 All relevant errors made by the Council must be reported to the Investigatory Powers Commissioner by the Council as soon as reasonably practicable and a full report provided no later than ten working days. The report should include information on the cause of the error; the amount of surveillance conducted, and material obtained or disclosed; any unintended collateral intrusion; any analysis or action taken; whether any material has been retained or destroyed; and a summary of the steps taken to prevent recurrence.

58.8 Serious Errors

58.9 The Investigatory Powers Commissioner must inform a person of any relevant error relating to that person if the Commissioner considers that the error is a serious error and that it is in the public interest for the person concerned to be informed of the error. The Commissioner may not decide that an error is a serious error unless they consider that the error has caused significant prejudice or harm to the person concerned. The fact that there has been a breach of a person's Convention rights (within the meaning of the HRA) is not sufficient by itself for an error to be a serious error.

59. Complaints

59.1 Any person who reasonably believes they have been adversely affected by surveillance activity by or on behalf of the Council may complain to the Council in accordance with the Council's Corporate Complaints and Representations Procedure.

59.2 Any person may also make a complaint to the official body, which is the IPT, about the Council using covert techniques against them. Details explaining how to make a complaint can be found on the IPT's website. The IPT has jurisdiction to investigate and determine complaints against the Council's use of RIPA powers, including those covered by this Policy.

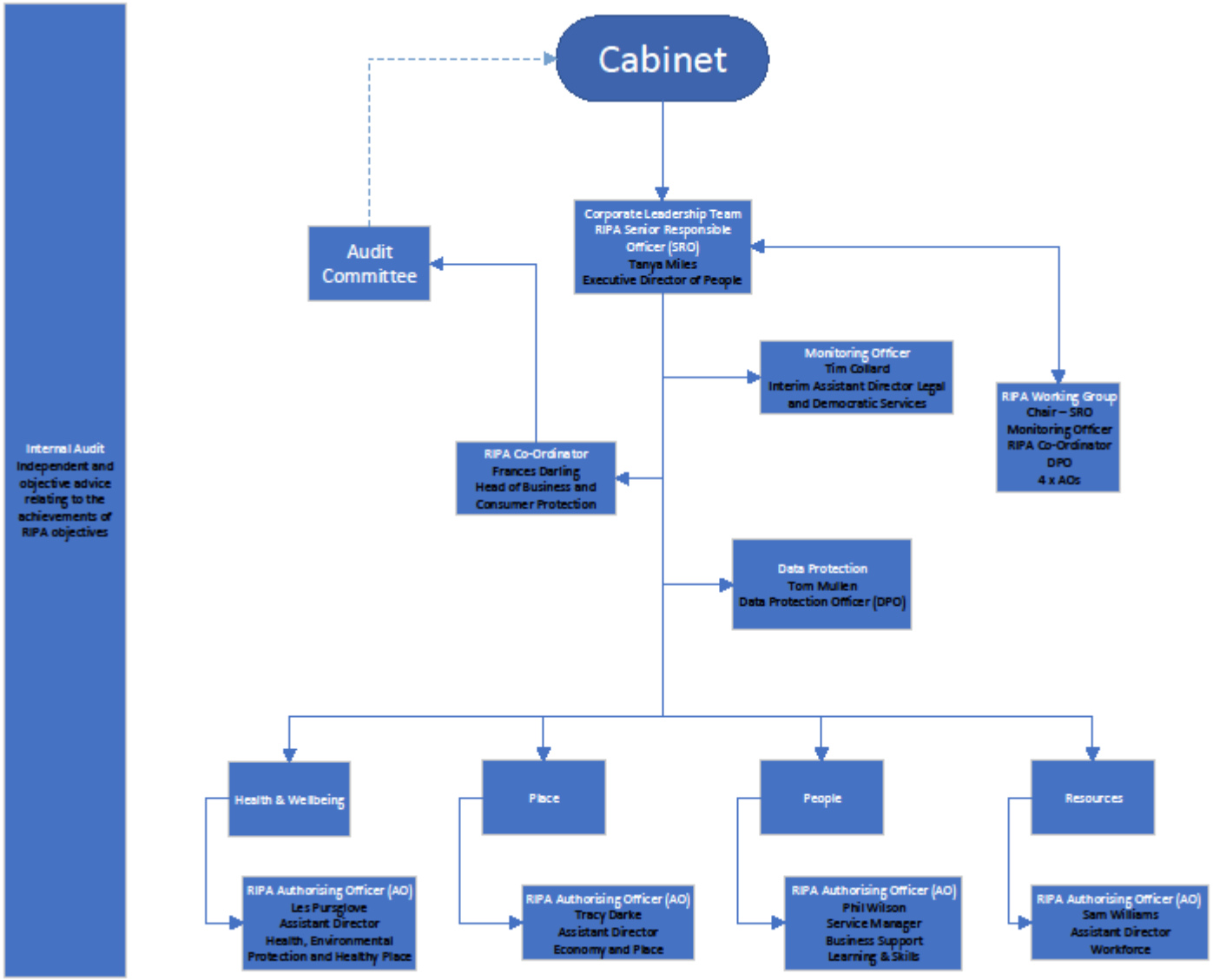
59.3 Complaints to the IPT should be:

Emailed to: info@ipt-uk.com

OR

Posted to: The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

APPENDIX A – Governance Structure



APPENDIX B – Designated Officers

Senior Responsible Officer: Tanya Miles, Executive Director of People

Monitoring Officer: Tim Collard, Interim Assistant Director Legal and Democratic Services

RIPA Coordinator: Frances Darling, Head of Business and Consumer Protection

Authorising Officers
The following officers are appointed to grant authorisations under Section 28 and 29 of RIPA, to verify communications data applications and to grant authorisations for 'non-RIPA' purposes (subject to appropriate training):

- Les Pursglove, Assistant Director Health, Environmental Protection and Healthy Place
- Tracy Darke, Assistant Director Economy and Place
- Phil Wilson, Service Manager Business Support Learning and Skills
- Sam Williams, Assistant Director Workforce
- Frances Darling, Head of Business and Consumer Protection (to undertake the role of an AO in exceptional circumstances, e.g. where no other AO is available)

APPENDIX C - Application and Authorisation Process

Relevant Forms

For both Directed Surveillance and CHIS authorisations there are six forms within the process. They are:

- Authorisation
- Application for Judicial Approval
- Judicial Approval Order
- Review
- Renewal
- Cancellation

All forms are available from the RIPA Coordinator.

Duration of Authorisations

Authorisations must be given for the maximum duration from the date approved by the JP but reviewed on a regular basis and formally cancelled when no longer needed. They do not expire; they must be cancelled when the surveillance is no longer proportionate or necessary. Therefore, a directed surveillance authorisation will cease to have effect after three months from the date of approval by the JP unless renewed or cancelled. The relevant durations are detailed below:

Directed Surveillance	3 Months
Renewal	3 Months
Covert Human Intelligence Source	12 Months
Renewal	12 months
Juvenile Sources	4 Months
Renewal	4 Months

It is the responsibility of the Investigating Officer to make sure that the authorisation is still valid when they undertake surveillance.

NB The expiry time on all authorisations is always at 23:59, e.g. an authorisation granted on 1 April 2021 at 16:54 will expire on 30 June 2021 at 23.59.

Applications/Authorisation

The applicant or another appropriate person must carry out a feasibility study and intrusion assessment as this may be required by the AO. The feasibility study aims to ensure that the surveillance operation is practically possible, that risks are minimised and limiting factors that may impede the success of the operation are managed. The person seeking the authorisation must then complete the application form having regard to the guidance given in this Policy and

the statutory Codes. There must not be any significant delay between the feasibility study and the completion of the application form to ensure that the details within the application are accurate and will not have changed. The form must then be submitted to the AO for authorisation.

When completing an application for authorisation, the applicant must ensure that the case for the authorisation is presented in the application in a fair and balanced way; in particular, all reasonable efforts should be made to take into account information which weakens the case for the warrant or authorisation. This is a requirement of the Codes.

All the relevant sections must be completed with sufficient information to ensure that applications are sufficiently detailed for the AO to consider necessity, proportionality having taken into account the collateral intrusion issues. Cutting and pasting or using template entries must not take place as this will leave the process open to challenge.

If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, the respective authorisations must be completed and the respective procedures followed. Both activities must be considered separately on their own merits.

Prior to an application being submitted to the AO, the Line Manager must perform an initial quality check of the application; however, they must not be involved in the sanctioning of the authorisation. All applications must be submitted by the applicant to the AO, with evidence confirming that the Line Manager for the team involved in the investigatory activity is aware of and supports the application. This is to ensure that the Line Manger is aware of the application and activities being undertaken by their staff.

Applications whether authorised or refused must be issued with a unique reference number. The number is obtained from the RIPA Coordinator by the Line Manager. The number will be generated by the RIPA Coordinator and must be an appropriate sequential number recorded in the central register.

If not authorised, feedback will be provided to the applicant and the application will be forwarded to the RIPA Coordinator for recording and filing. If, having received the feedback, the applicant feels it is appropriate to re-submit the application, they can do so and it will then be reconsidered.

Judicial approval process

With regard to the judicial approval process for RIPA, all officers involved in the authorisation process must familiarise themselves with the latest guidance available for local authorities in England and Wales.

Following authorisation, the applicant will then complete the relevant section of the judicial application/order form, which is available from the RIPA Coordinator. Although this form requires the applicant to provide a brief summary of the circumstances of the case, this is supplementary to and does not replace the need to also supply a copy and the original RIPA authorisation.

Where surveillance is used for non-RIPA purposes there is no requirement to obtain judicial approval.

Arranging the Court Hearing

The AO must contact or arrange for another officer on their behalf to contact Her Majesty's Courts and Tribunals Service (HMCTS) administration team at the appropriate Magistrates;' Court to arrange a hearing. The hearing will be in private and heard by a single JP. The application to the JP will be on oath.

Officers who may present the application at these proceedings will need to be formally designated by the Council under section 223 of the Local Government Act 1972 to appear, be sworn in and present evidence or information as required by the JP. If in doubt as to whether you are able to present the application seek advice from the RIPA Coordinator.

The application and judicial order forms to be used for judicial approval are available from the RIPA Coordinator.

Attending the Hearing

The applicant and the AO will attend the hearing, as the applicant cannot answer questions that relate to the AO's decision to grant an authorisation. It is, however, appropriate for the applicant to answer questions in relation to the detail of the case under investigation and for both parties to clarify matters relating to general policy and practice of conducting surveillance. It is not necessary to use a solicitor to make the case to a JP.

Upon attending the hearing, the applicant must present to the JP the partially completed judicial application/order form, the original and a copy of the RIPA application/authorisation form, together with any supporting documents setting out the case. The original RIPA authorisation must be shown to the JP but will be retained by the Council so that it is available for inspection by IPCO, and in the event of any legal challenge or investigations by the IPT.

The JP will read and consider the RIPA authorisation and the judicial application/order form**.** They may have questions to clarify points or require additional reassurance on particular matters. These questions are supplementary to the content of the application form. However, the forms and supporting papers must by themselves make the case. It is not sufficient for the Council to provide oral evidence where this is not reflected or supported in the papers provided.

The JP will consider whether they are satisfied that at the time the authorisation was granted or renewed, there were reasonable grounds for believing that the authorisation was necessary and proportionate. In addition, they must be satisfied that the person who granted the authorisation was an appropriate Designated Person within the Council to authorise the activity and the authorisation was made in accordance with any applicable legal restrictions, for example, the crime threshold for directed surveillance.

Decision of the Justice of the Peace (JP)

The JP has a number of options which are:

Approve or renew an authorisation. If approved by the JP, the date of the approval becomes the commencement date for the duration of the three months and the officers are now allowed to undertake the activity.

Refuse to approve or renew an authorisation. The RIPA authorisation will not take effect and the Council may **not** use the technique in that case.

Where an application has been refused, the applicant may wish to consider the reasons for that refusal. If more information was required by the JP to determine whether the authorisation has met the tests, and this is the reason for refusal, the officer should consider whether they can reapply, e.g. if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.

For a technical error (as defined by the JP), the form may be remedied without going through the internal authorisation process again. The officer may then wish to reapply for judicial approval once those steps have been taken.

Refuse to approve or renew and quash the authorisation. This applies where the JP refuses to approve or renew the authorisation and decides to quash the original authorisation. However, the court must not exercise its power to quash the authorisation unless the applicant has had at least two business days from the date of the refusal in which to make representations. If this is the case, the officer will inform Legal and Democratic Services and a solicitor will consider whether to make any representations.

The JP will record their decision on the order section of the judicial application/order form. The court administration will retain a copy of the Council's RIPA application and authorisation form and the judicial application/order form. The officer will retain the original authorisation and a copy of the judicial application/order form.

The Council may only appeal a JP decision on a point of law by judicial review. If such a concern arises, a solicitor from Legal and Democratic Services will decide what action, if any, should be taken.

Post Court Procedure

It will be necessary to work out the cancellation date from the date of approval and ensure that the applicant and the AO are aware. The original application and the copy of the judicial application/order form must be forwarded to the RIPA Coordinator. A copy will be retained by the applicant and, if necessary, by the AO. The central register will be updated with the relevant information to comply with the Codes and the original documents filed and stored securely.

Where dates are set within the process such as reviews, they must be adhered to. This will help with demonstrating that the process has been managed correctly in line with the Codes and reduce the risk of errors.

Reviews

When an application has been authorised and approved by a JP, regular reviews must be undertaken by the AO to assess the need for the surveillance to continue.

In each case the AO must determine how often a review needs to take place and set these at the outset. This decision will be based on the circumstances of each application and should be

as frequently as is considered necessary and practicable; however, it is recommended that they take place **at least** every month to ensure that the activity is properly managed.

Particular attention is drawn to the need to frequently review authorisations where the surveillance provides a high level of intrusion into private life or significant collateral intrusion, or confidential information. The AO will record, on the application form, when the reviews are to take place. It will be important for the AO to be aware of the review dates to ensure that the applicants submit the review form on time.

Applicants must submit a review form by the review date set by the AO. They must also use a review form for changes in circumstances to the original application which would include a change to the level of intrusion so that the need to continue the activity can be re-assessed. However, if the circumstances or the objectives have changed considerably, or the techniques to be used are now different, a new application form must be submitted, and it will be necessary to follow the process again and to be approved again by a JP. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances.

Line mangers of applicants must make themselves aware of when the reviews are required to ensure that the relevant forms are completed on time.

The reviews are dealt with internally by submitting the review form to the AO. There is no requirement for a review form to be submitted to a JP.

The results of a review must be recorded on the central record of authorisations.

A review of an authorisation is not the same as a renewal and AOs are directed to the section below and the relevant parts of the Codes to ensure the difference is fully understood and the principles correctly applied.

Renewal

A renewal form is to be completed by the applicant when the original authorisation period is about to expire but directed surveillance or the use of a CHIS is still required.

Should it be necessary to renew an authorisation for directed surveillance or a CHIS, this must be approved by a JP.

Applications for renewals should not be made until shortly before the original authorisation period is due to expire. However, they must take account of factors which may delay the renewal process, e.g. intervening weekends or the availability of the relevant AO and a JP to consider the application.

The applicant must complete all the sections within the renewal form and submit the form to the AO for consideration.

AOs must examine the circumstances with regard to necessity, proportionality and the collateral intrusion issues before making a decision to renew the activity. A CHIS application must not be renewed unless a thorough review has been carried out covering the use made of the source, the tasks given to them and information obtained. The AO must consider the results of the review when deciding whether to renew or not. The review and the consideration must be documented.

If the AO refuses to renew the application, the cancellation process must be completed. If the AO authorises the renewal of the activity, the same process is to be followed as mentioned earlier for the initial application whereby approval must be sought from a JP.

A renewal takes effect on the day on which the authorisation would have ceased and lasts for a further period of three months.

Authorisations may be renewed more than once if still considered necessary and proportionate and approved by a JP.

Cancellation

The cancellation form is to be submitted by the applicant or another investigator in their absence. The AO who granted or last renewed the authorisation must cancel it if they are satisfied that the directed surveillance no longer meets the criteria upon which it was authorised. Where the AO is no longer available, this duty will fall on the person who has taken over the role of AO or the person who is acting as AO. As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other investigating officer involved in the investigation must inform the AO. The AO will formally instruct the investigating officer to cease the surveillance, noting the time and date of their decision. This will be required for the cancellation form. The date and time when such an instruction was given must also be recorded in the central record of authorisations**.**

The Investigating Officer submitting the cancellation must complete in detail the relevant sections of the form and include the period of surveillance and detail if any images were obtained, particularly any images containing innocent third parties. The AO must take this into account and issue instructions regarding the management and disposal of the images, etc. (see sections 50 to 57).

The cancellation process must also be used to evaluate whether the objectives have been achieved and whether the applicant carried out what was authorised. This check will form part of the oversight function. Where issues are identified including errors (see section 58), they will be brought to the attention of the Line Manager and the SRO. This will assist with future audits and oversight and compliance with the Codes.

When cancelling a CHIS authorisation, an assessment of the welfare and safety of the source must also be assessed, and any issues identified.

All cancellations must be submitted to the RIPA Coordinator for inclusion in the Central Record and stored securely with the other associated forms.

Do not wait until the 3-month period has expired to cancel. Cancellation must be undertaken formally and promptly at the earliest opportunity once the surveillance has served its purpose or is no longer necessary and proportionate. Line Managers need to be aware of when the activity needs cancelling and ensure that staff comply with the procedure.