APPENDIX 1

Regulation of Investigatory Powers Act (RIPA) and non-RIPA Surveillance Policy

Draft

	RIPA (Regulation of Investigatory Powers Act 2000) and non-RIPA Surveillance Policy
Owner	**Nick Howard / Teri Munro**
Version	**1**
Issue Date	
Approved by	
Next revision due	**12 months from issue or sooner if Regulations or Legislation is amended**

This is a policy to ensure the Council complies with the Regulation of Investigatory Powers Act 2000 (RIPA) by ensuring there is a consistent approach to the authorisation process and undertaking of surveillance activity carried out by the Council.

Contents

Part A Introduction & RIPA General

1. Introduction

1.1 The performance of certain investigatory functions of local authorities may require the surveillance of individuals or the use of undercover officers and informants. Such actions may intrude on the privacy of individuals and can result in private information being obtained. The Regulation of Investigatory Powers Act 2000 (RIPA) governs these activities and provides a means of ensuring they are carried out in accordance with law and subject to safeguards against abuse.

1.2 All surveillance activity can pose a risk to the Council from challenges under the HRA or other processes. Therefore, it must be stressed that all staff involved in the process will take their responsibilities seriously which will assist with the integrity of the Council's processes, procedures, and oversight responsibilities.

1.3 In preparing this Policy, the Council has considered the RIPA Codes of Practice (August 2018).

1.4 The Council takes its statutory responsibilities seriously and will act in accordance with the law and the codes of practice.

2. Scope and Aim of the Policy

2.1 This Policy applies to all areas of the Council that may undertake enforcement action and / or carry out any form of surveillance activity.

2.2 The purpose of this Policy is to ensure the Council complies with the Regulation of Investigatory Powers Act 2000 (RIPA) by ensuring there is a consistent approach to the authorisation process and undertaking of surveillance activity carried out by the Council. This includes the use of undercover officers and informants, known as Covert Human Intelligence Sources (CHIS).

2.3 The policy also sets out the Council's position on surveillance which is necessary to be undertaken by the Council but cannot be authorised under the RIPA legislation. This is referred to as surveillance outside of RIPA and will have to be compliant with the Human Rights Act. (See section 'Surveillance Outside RIPA' paragraph 16).

2.4 All RIPA covert activity will have to be authorised and conducted in accordance with this Policy, the RIPA legislation, and Codes of Practice. Therefore, all officers involved in the process will have regard to this document and the statutory RIPA Codes of Practice issued under section 71 RIPA (current version issued in August 2018) for both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS). The Codes of Practice are available from the Home Office website.

2.5 This Policy and associated procedures also establish the Councils approach to ensure that all online research and investigations are conducted lawfully and ethically to reduce risk.

2.6 Failing to comply this Policy could result in Officers being dealt with through the Councils disciplinary procedures.

3. Background to RIPA and Lawful Criteria

3.1 The Human Rights Act 1998 (HRA) makes it potentially unlawful for a local authority to breach any article of the European Convention on Human Rights (ECHR).

3.2 Article 8 of the European Convention on Human Rights states that: -

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

II. There shall be no interference by the Council 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 can interfere with this right for the reasons given in 3.2 (ii) above, **if it is necessary and proportionate** to do so.

3.4 Those who undertake directed surveillance or CHIS activity on behalf of the Council breach an individual's Human Rights, unless such surveillance is lawful, consistent with Article 8 of the ECHR and is both necessary and proportionate to the matter being investigated.

3.5 RIPA provides the legal framework for lawful interference to ensure that any activity undertaken, together with the information obtained, is HRA compatible.

4. Consequences of Not Following RIPA

4.1 Although not obtaining authorisation does not make the surveillance unlawful per se, it does have some consequences: -

I. Evidence that is gathered may be inadmissible in court.

II. The subjects of surveillance can bring their own claim on Human Rights grounds i.e., the Council has infringed their rights under Article 8.

III. If a challenge under Article 8 is successful, the Council would receive reputational damage and could face a claim for financial compensation.

IV. The Government has also introduced a system of tribunal to deal with complaints. Any person who believes that their rights have been breached can have their complaint dealt with by the Investigatory Powers Tribunal (IPTC). (See section Errors and Complaints section F).

V. It is likely that the activity could be construed as an error and therefore must be investigated, and a report submitted by the Senior Responsible Officer to the Investigatory Powers Commissioner's Office (IPCO).

5. Independent Oversight

5.1 RIPA is overseen by the Investigatory Powers Commissioner's Office (IPCO). Their remit includes providing comprehensive oversight of the use of the powers to which the RIPA code applies, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes. To carry out their full functions and duties they will periodically inspect the records and procedures of the Council to ensure any authorisations have been given, reviewed, cancelled, and recorded properly. Therefore, it is important that the Council can show it complies with this Policy and with the provisions of RIPA.

5.2 The Codes of Practice require that as a local authority, the Council must report the fact of its use to elected council members. Members must be updated on a regular basis of any usage, or not, of the relevant powers. The Council will report its use, or non-use of these powers to members via the Performance & Governance Report on a six (6) monthly basis.

Part B. Surveillance, Types and Criteria

6. Surveillance Definition

6.1 There are several 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.

6.2 Surveillance is:

I. Monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications.

II. Recording anything monitored, observed, or listened to during surveillance, with or without the assistance of a device.

6 Training and Awareness

6.1 All staff need to be clear on the legal frameworks which govern their work, to ensure that the Council adheres to the relevant guidelines. Staff are urged to consider the implications of retention for any private data they obtain. Therefore, the Council will ensure that relevant staff are suitably trained for their role and responsibilities.

7. Overt and Covert Surveillance

7.1 **Overt surveillance** is where the subject of surveillance is aware it is taking place, either by way of signage such as in the use of CCTV (closed circuit television) or they have been informed of the activity. Overt surveillance is outside the scope of RIPA and therefore does not require authorisation. However, it still must take account of privacy under the Human Rights Act and be necessary and proportionate. Any personal data obtained will also be subject of the Data Protection Act. Overt CCTV cameras (fixed or portable) are also subject to both the Information Commissioners and Surveillance Camera codes of practice.

7.2 **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 (see below).

8. Intrusive Surveillance

8.1 The Council has no authority in law to carry out Intrusive Surveillance. It is only the Police and other law enforcement agencies that can lawfully carry out intrusive surveillance.

8.2 Intrusive surveillance is defined in section 26(3) of the 2000 Act as covert surveillance that:

I. Is carried out in relation to anything taking place on any residential premises or in any private vehicle; and

II. Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

8.3 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 present on the premises or in the vehicle. Thus, the observation of a premises or vehicles from the street or observation point which provides a limited view and no sound of what is happening inside the premises, would not be considered as intrusive surveillance

9. Directed Surveillance Definition

9.1 The Council can lawfully carry out Directed Surveillance. Surveillance is Directed Surveillance if the following are all true:

I. It is covert, but not intrusive surveillance.

II. It is conducted for the purposes of a specific investigation or operation.

III. It is likely to result in the obtaining of private information (see private information below) about a person (whether one specifically identified for the purposes of the investigation or operation).

IV. 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.

10. Private information

10.1 By its very nature, surveillance may involve invading an individual's right to privacy. The Code of Practice provides 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 can include any aspect of a person's private or personal relationship with others, such as family and professional or business relationships.

10.2 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by the Council of that person's activities for future consideration or analysis. Surveillance of publicly accessible areas of the internet should be treated in an equivalent 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.

10.3 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.

10.4 There is also an assessment to be made regarding the risk of obtaining collateral intrusion which relates to private information about persons who are not subjects of the surveillance This has a direct bearing when considering proportionality as part of the authorisation process.

11. Confidential or Privileged Material

11.1 This includes where the material contains information that is legally privileged, confidential journalistic material or where material identifies a journalist's source; 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 Managing Director or, whoever is deputising in their absence.

12. Lawful Grounds

12.1 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 a criminal offence(s) and includes actions taken to avert, end or disrupt the commission of criminal offences. It must also meet the serious crime test i.e., that the criminal offence(s) which is sought to be prevented or detected is:

I. Punishable, whether on summary conviction or on indictment, by a maximum term of at least 6 months of imprisonment, or,
II. 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 (see 1.4 above). This is the only ground available to the Council and hence the only justification.

12.2 Each application must be considered and authorised internally by an Authorising Officer from within the Council. Furthermore, the Council's authorisation can only take effect once an order approving the authorisation has been granted by a Magistrate of the Peace (JP).

12.3 RIPA ensures that any surveillance which is undertaken following authorisation and approval from a Magistrate of the Peace is lawful. Therefore, it protects the authority from legal challenge. It also renders evidence obtained lawful for all purposes.

13. Urgent cases

13.1 There is no provision to authorise urgent oral authorisations under RIPA for urgent cases as all authorisations must be approved by a Magistrate. If surveillance were required to be carried out in an urgent situation or as an immediate response, this would still have to be justified as necessary and proportionate under HRA. This type of surveillance is surveillance outside of RIPA. (See section 16 below).

14. CCTV and Automatic Number Plate Recognition (ANPR) Cameras.

14.1 The definition of CCTV is included under Section 29(6) Protection of Freedoms Act 2012 and "surveillance camera systems" is taken to include:

I. closed circuit television (CCTV) or automatic number plate recognition (ANPR) systems.
II. any other systems for recording or viewing visual images for surveillance purposes.
III. any systems for storing, receiving, transmitting, processing, or checking the images or information obtained by (a) or (b).
IV. any other systems associated with, or otherwise connected with (a), (b) or (c).

This includes:

I. Conventional town centre CCTV.
II. Body Worn Video (BWV).
III. Automatic Number Plate Recognition (ANPR).
IV. Deployable mobile **overt and covert** mobile camera systems.
V. Drones.

14.2 Surveillance camera systems are subject to both the Surveillance Camera Code of Practice and the Information Commissioners Office (ICO) CCTV Code of Practice titled 'In the Picture'.

14.3 The use of the conventional town centre CCTV systems and other overt cameras operated by the Council do not normally fall under the RIPA regulations. However, 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 an authorisation.

14.4 Operators of any of the Councils CCTV system need to be aware of the RIPA issues associated with using CCTV and other camera systems and that continued, prolonged systematic surveillance of an individual may require an authorisation.

14.5 On the occasions when the CCTV cameras are to be used in a Directed Surveillance situation either by enforcement officers from relevant departments within the Council or outside Law Enforcement Agencies such as the Police, the CCTV Policy should be followed where relevant as well as the RIPA Codes of Practice.

14.6 The same principles apply to Automated Number Plate Recognition (ANPR). Its use 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, if used in a pre-planned way to carry out covert surveillance which meets the RIPA criteria, this Policy and the codes of practice must be followed.

15. Internet and Social Media Investigations

15.1 Online open-source research is widely regarded as the collection, evaluation, and analysis of material from online sources available to the public, whether by payment or otherwise, to use as intelligence and evidence.

15.2 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 Human Rights Act (HRA) and other operational risks. Online open-source and social media research may breach someone's privacy. It may also meet the RIPA criteria and require authorising as per this Policy. Staff are to have regards to the privacy and RIPA issues detailed in the codes of practice and advice from IPCO.

15.3 Officer must be aware that any activity carried out over the internet leaves a trace or footprint that can identify the device used, and in some circumstances, the individual carrying out the activity.

15.4 There is also a risk of compromise to other investigations, therefore, the activity should be conducted in a manner that does not compromise any current or future investigation or tactics.

15.5 To justify the research being undertaken, there must be a clear lawful reason, and the research must be necessary. Therefore, 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 should be documented with clear objectives. Should the research fall within RIPA activity, the RIPA authorisation must detail these criteria for it to be lawful.

15.6 Whilst conducting the internet open-source research, the nature of the online activity may evolve. It is important staff 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.

16. Surveillance outside of RIPA

16.1 As already explained, for directed surveillance the criminal offence must carry a 6-month prison sentence (directed surveillance crime threshold) or relate to the sale of alcohol or tobacco to children. This means that there are investigation scenarios that do not meet this threshold, however it is necessary to undertake surveillance. This will fall outside of RIPA and examples include:

I. Surveillance for anti-social behaviour or disorder which do not attract a maximum custodial sentence of at least six months imprisonment.
II. Planning enforcement prior to the serving of a Notice or to establish whether a Notice has been breached.
III. Most licensing breaches.
IV. Safeguarding vulnerable people.
V. Civil matters.
VI. Disciplinary surveillance.

16.2 In the above scenarios, it is most probably to be targeted surveillance which is likely to breach someone's article 8 rights to privacy. Therefore, the activity should be conducted in a way which is HRA compliant, which will include it being necessary and proportionate.

16.3 As part of the process of formally recording and monitoring non-RIPA surveillance, non-RIPA surveillance forms are available, with the application and authorisation process being the same as for RIPA except it will not require to be approved by a Magistrate.

16.4 The Senior Responsible Officer (SRO) will maintain oversight of non-RIPA surveillance to ensure that such surveillance is compliant with Human Rights legislation.

17. Joint Agency and Third-Party Surveillance

17.1 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.

17.2 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 an agent to the Council and will be subject to RIPA in the same way as any employee of the Council would be.

17.3 Similarly, a surveillance authorisation should also be considered where the Council is aware that a third party (that is not a Public Authority) 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.

Part C. Covert Human Intelligence Sources (CHIS)

18 Introduction

18.1 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.

18.2 The lawful grounds for CHIS authorisation are the prevention and detection of crime and prevention of disorder. The serious crime criteria of the offence carrying a 6-month sentence etc. **does not apply to CHIS.**

18.3 Recognising when a source becomes a CHIS is therefore important as this type of activity may need authorisation. Should a CHIS authority be required, all staff involved in the process should make themselves fully aware of the contents of this Policy and the CHIS codes of practice.

19. Definition of CHIS

19.1 Individuals act as a covert human intelligence source (CHIS) if they:

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

19.2 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. This does not mean the relationship with the Council officer and the person providing the information, as this is not covert. It relates to how the information was either obtained or will be obtained. Was it or will it be obtained from a third party without them knowing it was being passed on to the Council? If the answer is yes, this would amount to a covert relationship.

19.3 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 should be considered, for example, where the Council is aware that a third party is independently maintaining a relationship (e.g., “self-tasking”) to obtain evidence of criminal activity, and the Council intends to make use of that material for its own investigative purposes. (Section 2.26 Codes of CHIS Codes of Practice.

20. Vulnerable and juvenile CHIS

20.1 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 need community care services by reason of mental or other disability, age, or illness and who is or may be unable to take care of himself, or unable to protect himself 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 Managing Director (or, in their absence, whoever is the designated deputy).

20.2 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 his parents or any person who has parental responsibility for him. 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.

21. Risk Assessments

21.1 The Council has a responsibility for the safety and welfare of the source and as detailed in the codes of practice, a risk assessment will be conducted, and all the guidance contained within the codes will be followed.

Part D. Roles and Responsibilities

22 The Senior Responsible Officer (SRO)

22.1 The nominated Senior Responsible Officer Assistant Director – Regulatory. (See Appendix A). The SRO has responsibility for:

i. The integrity of the process in place within the Council to authorise directed and intrusive surveillance.
ii. Compliance with the relevant sections of RIPA and the Codes of Practice.
iii. Oversight of the reporting of errors to the Investigatory Powers Commissioner (IPC) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors.
iv. Engagement with the Investigatory Powers Commissioner Office (IPCO) and the inspectors who support the Commissioner when they conduct their inspections.
v. Where necessary, overseeing the implementation of any recommended post-inspection action plans.
vi. Ensuring that all Authorising Officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner.

23. RIPA Co-ordinator (RCO)

23.1 The RCO is the Community Safety & Interventions Lead (see appendix A).

The RCO is responsible for storing all the 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 Authorising Officer or refused by a JP.

23.2 The RCO will: -

I. Keep the copies of the forms (listed above) for a period of at least 5 years.
II. Keep the Central Register (a requirement of the Codes of Practice) of all authorisations, renewals, and cancellations; and issue the unique reference number. This will also identify and monitor expiry and renewal dates.
III. Must ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Councils Retention Policy, departmental retention schedules and the Data Protection Act 2008. (DPA).
IV. Provide administrative support and guidance on the processes involved.
V. Monitor the authorisations, renewals, and cancellations with a view to ensuring consistency throughout the Council.
VI. Monitor each department's compliance and act on any cases of non-compliance.
VII. Provide or identify training and further guidance and awareness of RIPA and the provisions of this Policy; and review the contents of this Policy.

24. Authorising Officers

24.1 The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 prescribes that for Local Authorities, the Authorising Officer shall be a Director, Head of Service, Service Manager or equivalent as distinct from the officer responsible for the conduct of an investigation. Authorising Officers within the Council who can grant authorisations are at Senior Manager level. (See appendix A).

24.2 Authorising Officers **will not** authorise any documents relating to investigations or operations in which they are directly involved by directing, managing or otherwise playing a part. The role of the Authorising Officers is to consider whether to authorise, review, or renew an

authorisation. They must also officially cancel the RIPA covert activity. Authorising Officers must have been trained to an appropriate level to understand the requirements in the Codes of Practice that must be satisfied before an authorisation can be granted.

25 Necessity and Proportionality

25.1 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.

25.2 The Authorising Officer must believe the authorisation is necessary in the circumstances of the case and meets one or more of the statutory grounds. For the Council to use directed surveillance, those grounds are the prevention and detection of crime, and that the crime attracts a custodial sentence of a maximum of 6 months or more; or for the purpose of preventing or detecting specified criminal offences relating to the underage sale of alcohol and tobacco.

25.3 The lawful criteria for CHIS are prevention and detection of crime and prevention of disorder and the offence does not have to have a sentence of 6 months imprisonment.

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

24.5 If the activities are deemed necessary, the Authorising Officer 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 which is collateral intrusion) against the need for the activity in investigative and operational terms. The authorisation will not be proportionate if it is excessive in the overall circumstances of the case.

26. Collateral Intrusion

26.1 The Authorising Officer should also consider the risk of obtaining collateral intrusion which is private information about persons who are not subjects of the surveillance. Staff should take measures, wherever practicable, to avoid or minimise unnecessary intrusion into the privacy of those who are not the intended subjects of the surveillance.

27 Forms and Durations

27.1 For both directed surveillance and CHIS authorisations there are several forms within the process. They are:

I. Authorisation.
II. Review.
III. Renewal.
IV. Cancellation.
V. Magistrates Form.

27.2 Authorisations must be given for the maximum duration from the date approved by the JP/Magistrate 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. No surveillance etc. can be undertaken after the expiry date unless renewed and approved by the Magistrate. Durations detailed below:

I.	Directed Surveillance	3 Months
II.	Renewal	3 Months

III.	Covert Human Intelligence Source	12 Months
IV.	Renewal	12 months
V.	Juvenile Sources	4 Months
VI.	Renewal	4 Months

27.3 These durations also apply to any surveillance activities undertaken outside of RIPA.

27.4 The relevant application forms will be drawn directly from the Home Office website.

27.5 The relevant application forms for surveillance activities outside of RIPA will be maintained on Connect.

27.6 A separate restricted procedure document detailing the whole of the application and operational information will be maintained.

Part E Central Record and safeguarding the material

28. Central Record

28.1 The Council will maintain a centrally retrievable record of all authorisations/refusals which will be held and maintained by the RCO. 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.

28.2 The documents contained in the centrally held register should be retained for at least five years from the ending of the authorisation or for the period stipulated by the Council's Retention Policy, whichever is greater. The centrally held register will contain the following information:

I. If refused, (the application was not authorised by the AO) a brief explanation of the reason. The refused application should be retained as part of the central record of authorisation.
II. If granted, the type of authorisation and the date the authorisation was given.
III. 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.
IV. Name and job title of the authorising officer.
V. The unique reference number (URN) of the investigation or operation.
VI. The title of the investigation or operation (if there is one), including a brief description and names of subjects, if known.
VII. Frequency and the result of each review of the authorisation.
VIII. If the authorisation is renewed, when it was renewed and who authorised the renewal, including the name and grade of the authorising officer and the date renewed by the JP.
IX. Whether the investigation or operation is likely to result in obtaining confidential information as defined in this code of practice.
X. The date the authorisation was cancelled.
XI. Authorisations by an Authorising Officer where they are directly involved in the investigation or operation. If this has taken place it must be brought to the attention of a commissioner or Inspector during their next RIPA inspection.

28.3 As well as the central record, the Council will also retain:

I. 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 Authorising Officer.
II. The frequency and result of reviews prescribed by the Authorising Officer.

III. The date and time when any instruction to cease surveillance was given.
IV. The date and time when any other instruction was given by the Authorising Officer.
V. A record of the period over which the surveillance has taken place. This should have been included within the cancellation form.

28.4 Detailed records must be kept of the authorisation and the use made of a CHIS. The Regulation of Investigatory Powers (Source Records) Regulations 2000; SI No: 2725 details the particulars that must be included in these records. The Council will comply with these requirements.

29. Safeguarding the use of surveillance and CHIS material

29.1 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.

29.2 The Council should ensure that their actions when handling information obtained by means of covert surveillance or CHIS activity, comply with relevant legal frameworks and in particular, Chapter 9 'Safeguards (including privileged or confidential information)' of the Codes of Practice, so that any interference with privacy is justified in accordance with Article 8(2) of the European Convention on Human Rights. 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 Criminal Procedures Investigations Act (CPIA) and the DPA.

30. Authorised Purpose

30.1 Dissemination, copying and retention of material must be limited to the minimum necessary or an authorised purpose. Something is necessary for the authorised purposes if the material:

I. Is, or is likely to become, necessary for any of the statutory purposes set out in the RIPA Act in relation to covert surveillance or CHIS activity.
II. Is necessary for facilitating the carrying out of the functions of public authorities under RIPA.
III. Is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal.
IV. Is necessary for the purposes of legal proceedings.
V. Is necessary for the performance of the functions of any person by or under any enactment.

31. Use of Material as Evidence

31.1 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 Criminal Procedure, and Investigations Act 1996 (CPIA), the Civil Procedure Rules, section 78 of the Police and Criminal Evidence Act 1996 and the Human Rights Act 1998.

31.2 There is nothing in RIPA which prevents material obtained under directed surveillance authorisations from being used to further other investigations.

32. Dissemination of Information

32.1 It may be necessary to disseminate material acquired through the RIPA covert activity. The number of persons to whom any of the information is disclosed, and the extent of disclosure, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out in section 30 above. It will be necessary to consider exactly what and how

much information should be disclosed. Only so much of the material may be disclosed as the recipient needs; for example, if a summary of the material will suffice, no more than that should be disclosed.

32.2 The obligations apply not just 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.

32.3 A record will be maintained justifying any dissemination of material. If in doubt, seek advice from the Data Protection Officer.

33. Storage, Copying and Destruction

33.1 Material obtained through covert surveillance and CHIS authorisations, and all copies, extracts, and summaries of it, must be handled and stored securely, to minimise the risk of loss. It must be held 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.

33.2 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.

33.3 During an investigation, Council Officers 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.

33.4 Information obtained through covert surveillance, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction, and securely destroyed as soon as they are no longer needed for the authorised purpose(s) set out above. If such information is retained, it should 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

34. Errors

34.1 Errors relating to the RIPA process can have consequences to 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. There is a process detailed within the codes of practice relating to errors.

There are two types of errors within the codes of practice which are:

1. Relevant error.
2. Serious error.

Examples of relevant errors would include circumstances where:

I. Surveillance activity has taken place without lawful authorisation.

II. There has been a failure to adhere to the safeguards set out in the relevant statutory provisions and Chapter 9 of the Surveillance Codes of Practice relating to the safeguards of the material.

34.2 The Council will comply with the procedures set out in the Codes by establishing whether the error is a relevant error and if so, report it to the IPCO who will determine whether it is a serious error and what action is to be taken. A serious error is one that has caused significant prejudice or harm to the person concerned.

35 Complaints

35.1 Any person who believes they have been adversely affected by surveillance activity by or on behalf of the Council, may complain using the council's complaint procedure.

A complaint can also be made to the official body which is the Investigatory Powers Tribunal (IPT). The IPT has the authority to investigate and determine complaints against a public authority's use of RIPA powers, including those covered by this Policy.

Complaints should be addressed to:

The Investigatory Powers Tribunal
PO Box 33220
London
SWIH 9ZQ

This Policy should not be exempt from disclosure under the Freedom of Information Act 2000.