Version Control:	
Document Name:	Regulation of Investigatory Powers Act 2000 Surveillance and Covert Human Intelligence Source Policy
Version:	2.1
Responsible Officer:	Emma Cathcart, Counter Fraud and Enforcement Unit
Approved by:	Cabinet / Executive / Audit & Standards Committee
Next Review Date	January 2024
Retention Period:	N/A

Revision History

Revision date	Version	Description
April 2019 – April 2021	2	Change in legislation / introduction of IPA 2016
November 2021	2.1	Reference to CHIS (Criminal Conduct) Act 2021

Consultees

Internal	External
Enforcement Lead Officers Governance Groups One Legal / Legal Services Corporate / Executive / Senior Leadership Audit / Audit and Governance / Audit, Compliance and Governance Committee	Investigatory Powers Commissioner's Office

Distribution

Name	
Enforcement Officers	

CONTENTS

1. INTRODUCTION

1.1 The performance of certain investigatory functions by 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 and as such, should not be undertaken without full and proper consideration. The Regulation of Investigatory Powers Act 2000 (RIPA) regulates these types of activities and the Act and this Policy must be followed at all times.

1.2 Neither RIPA nor this Policy covers the use of any overt surveillance, or general observation that forms part of the normal day to day duties of Officers, or circumstances where members of the public volunteer information to the Council. The majority of the Council's enforcement functions are carried out in an overt manner.

1.3 RIPA was introduced to ensure that public authorities' actions are consistent with the Human Rights Act 1998 (HRA). It balances safeguarding the rights of the individual against the needs of society as a whole to be protected from crime and other public safety risks. This reflects the requirements of Article 8 (right to privacy) under the HRA. RIPA provides a statutory mechanism for authorising covert surveillance and the use of a covert human intelligence source (CHIS).

1.4 RIPA also introduced a legal gateway for public authorities to apply for telecommunications and postal data. However, these have been amended by the Investigatory Powers Act 2016 (IPA), and for guidance in relation to the obtaining of Communications Data please see the IPA Acquisition of Communications Data Policy.

2. SCOPE OF POLICY

2.1 The purpose of this document is to ensure that the Council complies with RIPA.

2.2 This document provides guidance on the regulation of any Directed Covert Surveillance that is carried out by the Council. This includes the use of undercover Officers and informants, known as Covert Human Intelligence Sources (CHIS).

2.3 Covert surveillance will only be used by the Council where it judges such use to be necessary and proportionate to the seriousness of the crime or matter being investigated.

2.4 All directed surveillance must be authorised and conducted in accordance with RIPA. Therefore, all Officers involved in the process must have regard to this document and the statutory Codes of Practice issued under section 71 RIPA. The Codes of Practice are available from:

https://www.gov.uk/government/collections/ripa-codes#current-codes-of-practice

2.5 There must be no situation where a Council Officer engages in covert surveillance without obtaining authorisation in accordance with the procedures set out in this document and the RIPA Codes of Practice.

2.6 Any queries concerning the content of the document should be addressed to the RIPA Coordinator, Counter Fraud Unit.

3. BACKGROUND

3.1 RIPA provides a legal framework for the control and regulation of covert surveillance techniques which public authorities undertake as part of their duties. As was highlighted in the introduction to this Policy, the need for such control arose

as a result of the HRA. Article 8 of the European Convention on Human Rights states that:-

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

2) 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.

3.2 The right under Article 8 is a qualified right and public authorities can interfere with this right for the reasons given in 2.3 above. RIPA provides the legal framework for lawful interference.

3.3 However, under RIPA, Local Authorities can only authorise directed covert surveillance for the purpose of preventing or detecting conduct which constitutes a criminal offence which is:

- An offence that is capable of attracting a maximum prison sentence of 6 months or more punishable whether on summary conviction or indictment meets the serious crime threshold or,
- Relates to the underage sale of alcohol or tobacco.

3.4 Furthermore, the Council's authorisation can only be given effect once an Order approving the authorisation has been granted by a Justice of the Peace (JP).

3.5 The serious crime criteria do not apply to CHIS authorisations.

3.6 RIPA ensures that any surveillance undertaken following a correct authorisation and approval from a JP is lawful and therefore protects the Council from legal challenge. It allows the information obtained to be used as evidence in the investigation. It can also be used if required in other investigations.

4. SURVEILLANCE WITHOUT RIPA

4.1 Section 27 of RIPA provides that surveillance shall be lawful for all purposes if authorised and conducted in accordance with an authorisation granted under RIPA.

4.2 Lawful surveillance is exempted from civil liability.

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

- Evidence that is gathered may be inadmissible in court;
- The subjects of surveillance can bring their own proceedings or defeat proceedings brought by the Council against them on human rights grounds i.e. we have infringed their rights under Article 8;
- If a challenge under Article 8 is successful, the Council could face a claim for financial compensation;
- 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 Complaints section within the Code of Practice)

5. INDEPENDENT OVERSIGHT

5.1 From 1 September 2017 oversight of RIPA is provided by the Investigatory Powers Commissioner's Office (IPCO). They are the independent inspection office whose remit includes providing comprehensive oversight of the use of the powers to which the RIPA Codes of Practice apply, and adherence to the practices and processes described in it. They also provide guidance to be followed which is separate to the codes.

5.2 Anyone, including anyone working for the Council, who has concerns about the way that investigatory powers are being used, may report their concerns to the IPCO

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

5.4 It is the duty of any person who uses these powers to comply with any request made by a Commissioner to disclose or provide any information required for the purpose of enabling them to carry out their functions.

5.5 It is important that the Council can show it complies with this Policy and with the provisions of RIPA.

6. LEGAL ADVICE

6.1 The Council's legal representatives will provide legal advice to staff making, renewing or cancelling authorisations. Requests and responses for legal advice will be in writing and copied to the RIPA Coordinator, Counter Fraud Unit to keep on file.

7. REVIEW OF POLICY AND PROCEDURE

7.1 The Audit Committee will receive annual reports regarding the use of RIPA. Those reports will contain information on:

- Where and when the powers have been used;
- The objective;
- The authorisation process;
- The job title of the Senior Responsible Officer (SRO), Authorising Officers (AO) and RIPA Coordinator;
- The outcomes including any legal court case;
- Any costs.

8. RIPA ROLES AND RESPONSIBILITIES

8.1 THE SENIOR RESPONSIBLE OFFICER

8.2 The SRO has responsibility for the following:

- The integrity of the process in place within the Council to authorise Directed and Intrusive Surveillance;

- Compliance with the relevant sections of RIPA and the Codes of Practice;
- 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;
- Engagement with the IPCO and the inspectors who support the IPC when they conduct their inspections;
- Where necessary, overseeing the implementation of any recommended post-inspection action plans and;
- Ensuring that all AO are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the IPC.

8.3 THE RIPA COORDINATOR

8.4 The RIPA Coordinator 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 the AO or refused by a JP.

8.5 The RIPA Coordinator will:

- Keep the copies of the forms for a period of at least 3 years;
- Keep the Central Register (a requirement of the Codes of Practice) of all of the authorisations, renewals and cancellations; and issue a unique reference number. This record should contain the information outlined within the Covert Surveillance and Property Interference revised Code of Practice;
- Keep a database for identifying and monitoring expiry dates and renewal dates;
- Along with Officers (AO and Investigating Officers (IO)), ensure that any electronic and paper records relating to a RIPA investigation are used, retained or destroyed in line with the Council's Information Management Policies, Departmental Retention Schedules and Data Protection Legislation /Regulations;
- Provide administrative support and guidance on the processes involved;
- Not provide legal guidance or advice;
- Monitor the authorisations, renewals and cancellations with a view to ensuring consistency throughout the Council;
- Monitor each department's compliance and act on any cases of non-compliance;
- Provide training and further guidance and awareness of RIPA and the provisions of this Policy; and review the contents of this Policy.

8.6 INVESTIGATING OFFICER/APPLICANT

8.7 The applicant is normally an IO who completes the application section of the RIPA form. IOs should think about the need to undertake directed surveillance or the use of a CHIS before they seek authorisation. IOs must consider whether they can obtain the information by using techniques other than covert surveillance. Advice can be given by the RIPA Coordinator.

8.8 The applicant or IO must carry out a feasibility study and this should be seen by the AO. The IO seeking authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any significant delay between the feasibility study and the completion of the application form in order to ensure that the details within the application are accurate. The form should then be submitted to the AO for authorisation.

8.9 AUTHORISING OFFICERS

8.10 The role of the AO is to authorise, review, renew and cancel directed surveillance.

8.11 AOs should not be responsible for authorising investigations or operations in which they are directly involved. Where an AO authorises such an investigation or operation the Central Record of Authorisations should highlight this, and it should be brought to the attention of the Inspector during their next inspection.

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

8.13 A designated AO must qualify both by rank and by competence. Officers who wish to be designated must have been trained to an appropriate level in order to have an understanding of RIPA and the requirements that must be satisfied before an authorisation can be granted.

8.14 Authorisations must be given in writing by the AO by completing the relevant section on the authorisation form. Before giving authorisation for directed surveillance, an AO must be satisfied that the reason for the request is for the prevention and detection of crime and that the crime attracts a custodial sentence of a maximum of 6 months or more, or is an offence relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

8.15 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 but consideration must be given to the risk of collateral intrusion (the risk of obtaining private information about persons who are not the subject of investigation), the possibility of collecting confidential personal information and that the result cannot reasonably be achieved by any other means.

8.16 When completing an authorisation, the case should be presented 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 authorisation.

8.17 The application should explain why the activity is both necessary and proportionate, having regard to the collateral intrusion. It should also explain exactly what is being authorised, against whom, in what circumstances, where and so on, and that the level of the surveillance is appropriate to achieve the objectives. It is important that this is very clear as the surveillance operatives will only be able to carry out activity that has been authorised. This will assist with avoiding errors.

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

8.19 The AO may be required to attend court to explain what has been authorised and why. Alternatively, they may have to justify their actions at a tribunal. AOs are also responsible for carrying out regular reviews of applications, for authorising renewals and cancelling any authorisation (see relevant sections below).

8.20 AOs must acquaint themselves with the relevant Codes of Practice issued by the Home Office regarding RIPA and the current Procedures and Guidance issued by the Commissioner. This document also details the latest operational guidance to be followed. It is recommended that AOs hold their own copy of this document.

8.21 AOs, through the Council's Data Controller, must ensure compliance with the appropriate data protection requirements under data protection legislation and regulation and any relevant internal protocols of the Council relating to the handling and storage of material.

9. SURVEILLANCE TYPES AND CRITERIA

9.1 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.

9.2 By its very nature, surveillance may involve invading an individual's right to privacy. The level of privacy which individuals can expect depends upon the nature of the environment they are within at the time. For example, 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 out into public areas.

9.3 There are different types of surveillance which, depending on their nature, are either allowable or not allowable and that require different degrees of authorisation and monitoring under RIPA.

9.4 OVERT SURVEILLANCE

9.5 Overt surveillance is where the subject of surveillance is aware that it is taking place. This could be by way of signage, such as in the use of CCTV, or because 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 still must take account of privacy under the HRA.

9.6 COVERT SURVEILLANCE

9.7 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.

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

1) **Directed Surveillance;**
2) **Covert Human Intelligence Sources** (CHIS); and
3) **Intrusive surveillance** (the Council is not permitted to carry out intrusive surveillance).

9.9 INTRUSIVE SURVEILLANCE

9.10 The Council has no authority in law to carry out Intrusive Surveillance. Intrusive surveillance is defined in section 26(3) of 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.

9.11 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.

9.12 A risk assessment of the capability of equipment being used for surveillance of residential premises and private vehicles should be carried out to ensure that it does not fall into intrusive surveillance.

9.13 If you are considering conducting surveillance that may fall within the scope of intrusive surveillance you must contact the RIPA Coordinator for clarification or seek legal advice from the legal department before you undertake any surveillance.

9.14 DIRECTED SURVEILLANCE

9.15 Surveillance is directed surveillance within RIPA if the following are applicable:

- 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 (see private information below) about a person (whether or not one specifically identified for the purposes of the investigation or operation);
- 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.
- The offence under investigation attracts a maximum custodial sentence of six months, or it is an investigation into criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

10. PRIVATE INFORMATION

10.1 The Code of Practice provides guidance on the definition of private information and states it includes any information relating to a person's private or family life. As a result, private information is capable of comprising any aspect of a person's relationship with others including family and professional or business relationships.

10.2 Information which is non-private may include publicly available information such as books, newspapers, journals, TV and radio broadcasts, newswires, web sites, 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.

10.3 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 though acting in public, and where a record is being made by the Council of that person's activities for future consideration or analysis.

10.4 Surveillance of publicly accessible areas of the internet should be treated in a similar way particularly when accessing information on social media websites. (See the Internet and Social Media Research and Investigations Policy for further guidance)

10.5 Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish a pattern of behaviour. Consideration must be given if one or more pieces of information (whether or not available in the public domain) are covertly and / or 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.

10.6 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

11. CONFIDENTIAL OR PRIVILEGED MATERIAL

11.1 Particular consideration should 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 material containing 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 Head of Paid Service, or (in their absence) the person acting as the Head of Paid Service (as per the codes and Statutory Instrument). Advice should be sought from the RIPA Coordinator and the Legal Department if there is a likelihood of this occurring.

12. INTERNET AND SOCIAL MEDIA INVESTIGATIONS

12.1 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.

12.2 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 Human Rights Act (HRA) and other operational risks. The activity may also require RIPA authorisations for Directed Surveillance or CHIS. Where this is the case, the application process and the contents of this policy are to be followed.

12.3 There is a detailed Internet and Social Media Research and Investigations Policy that covers online open source research which should be read and followed in conjunction with this policy.

13. CCTV

13.1 The use of the CCTV systems operated by the Council does not normally fall under the RIPA regulations. However, it does fall under the data protection legislation and regulations, the Surveillance Camera Code 2013 and the Council's CCTV Policy. 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 under RIPA. The Council's CCTV Policy and Procedures should be referred to.

13.2 If an IO envisages using any other CCTV system they should contact the RIPA Coordinator concerning any clarification on the administrative process or seek legal advice before they undertake any surveillance.

14. AUTOMATIC NUMBER PLATE RECOGNITION (ANPR)

14.1 Automated 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 or by plotting its locations, e.g. in connection with illegally disposing of waste.

14.2 Should it be necessary to use the Police ANPR systems to monitor vehicles, the same RIPA principles apply regarding when a directed surveillance authorisation should be sought.

15. JOINT AGENCY SURVEILLANCE

15.1 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.

15.2 Council staff involved with joint agency surveillance must ensure that all parties taking part are authorised on the form to carry out the activity. When Council Officers 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 should also provide a copy of the authorisation to the RIPA Coordinator at the Council to assist with oversight and monitoring.

16. USE OF THIRD PARTY AGENTS

16.1 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 should be authorised. The agent will be subject to RIPA in the same way as any employee of the Council would be. The AO should ensure that the agents are qualified or have the necessary skills to achieve the objectives. They should also ensure that they understand their obligations under RIPA. If advice is required, please contact the Legal Department.

16.2 If the above circumstances apply and it is intended to instruct an agent to carry out the covert activity, the agent must complete and sign the appropriate form.

16.3 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 or is to act as the prosecuting body.

17. EQUIPMENT

17.1 All equipment capable of being used for directed surveillance, such as cameras, should be fit for the purpose for which they are intended. The equipment should be logged on the central register of equipment held by the RIPA Coordinator. This will require a description, Serial Number, and an explanation of its capabilities.

17.2 When completing an Authorisation, 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 and proportionality. The AO must make it clear on the Authorisation exactly what equipment, if any, they are authorising and under what circumstances.

18. COVERT HUMAN INTELLIGENCE SOURCES (CHIS)

18.1 This policy applies to all use of under-cover Officers or informants, referred to as Covert Human Intelligence Sources (CHIS). 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 a professional or statutory duty or has been tasked to obtain information other than by way of a covert relationship.

18.2 Test purchase activity does not in general require authorisation under RIPA as vendor-purchaser activity does not constitute a relationship. However, if a number of visits are undertaken, a relationship may be established and authorisation as a CHIS should be considered. Equally a test purchase may meet the definition of directed surveillance.

18.3 If you intend to instruct a third party to act as the CHIS, the agent must complete and sign the appropriate form. The agent will be subject to RIPA in the same way as any employee of the Council would be. If advice is required, please contact either the RIPA Coordinator or the Legal Department.

18.4 An application for either directed surveillance or the use of a CHIS will need authorising internally by an AO. If authorised by the AO, approval will be required from a Justice of the Peace (JP) prior to any activity taking place. (See the appropriate sections below).

18.5 The authorisation request should be accompanied by a risk assessment, giving details of how the CHIS is going to be handled and the arrangements which are in place for ensuring that there is at all times a person with responsibility for

maintaining a record of the use made of CHIS. The risk assessment should take into account the safety and welfare of the CHIS in relation to the activity and should 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 should also be considered at the outset.

18.6 Where surveillance or the use of a CHIS is likely to result in the obtaining of confidential information, it is imperative that legal advice should first be sought from the SRO or the Legal Department. Confidential information includes, though is not limited to, matters subject to legal privilege, confidential personal information and confidential journalistic material. Confidential personal information is information held in confidence relating to the physical or mental health or spiritual counselling concerning an individual (whether living or dead) who can be identified from it.

18.7 Should a CHIS authority be required, all of the staff involved in the process should make themselves fully aware of all of the aspects relating to tasking contained within the CHIS codes of Practice.

18.8 Legal advice should always be sought where consideration is given to the use of CHIS.

18.9 DEFINITION OF CHIS

18.10 A CHIS is a person who: -

- Establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within the following paragraphs;
- Covertly uses such a relationship to obtain information or to provide access to any information to another person; or
- Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

18.11 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.

18.12 The serious crime criteria of the offences under investigation do not apply to CHIS.

18.13 CHIS's 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 IO,
- That there will at all times be another Officer within the Council who will have general oversight of the use made of the source; (controller) i.e. the 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.
- That the records relating to the source maintained by the local authority will always contain particulars of all matters specified by the Secretary of State in Regulations.

18.14 The Handler will have day to day responsibility for:

- dealing with the source on behalf of the Council concerned;

- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare.

18.15 The Controller will be responsible for the general oversight of the use of the source.

18.16 Tasking is the assignment given to the source by the Handler or Controller such as asking them to obtain information, to provide access to information or to otherwise act, incidentally, for the benefit of the relevant 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.

18.17 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. For example, 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. Other authorisations under the Act, for example, directed surveillance, may need to be considered where there is a possible interference with the Article 8 rights of an individual.

18.18 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.

18.19 VULNERABLE CHIS

18.20 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 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 by the Head of Paid Service, or (in their absence) the person acting as the Head of Paid Service (as per the codes and Statutory Instrument).

18.21 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 them.

18.22 If the use of a Vulnerable Individual or a Juvenile is being considered as a CHIS you must consult the Legal Department before authorisation is sought as authorisations should not be granted unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) Order 2000; SI No. 2793 are satisfied. Authorisations for Juvenile Sources must be authorised by the by the Head of Paid Service, or (in their absence) the person acting as the Head of Paid Service (as per the codes and Statutory Instrument).

18.23 It is unlikely that the use of a Vulnerable Individual or Juvenile CHIS by the Council will meet the requirements of necessity and proportionality and be considered justifiable.

18.24 USE OF EQUIPMENT BY A CHIS

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

18.26 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 inside those premises or that vehicle which takes place in their presence. This also applies to the recording of telephone conversations.

18.27 CHIS MANAGEMENT

18.28 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 on an ongoing basis to ensure the operation remains proportionate. The security and welfare of the source will also be monitored. The AO should maintain general oversight of these functions.

18.29 During CHIS activity there may be occasions when unforeseen action or undertakings occur. Such incidences should be recorded as soon as practicable after the event and if the existing authorisation is insufficient, it should either be dealt with by way of a review and updated (for minor amendments only) or it should be cancelled, and a new authorisation obtained before any further action is carried out. Similarly, where it is intended to task a CHIS in a new significantly different way than previously identified, the proposed tasking should be referred to the AO, who should consider whether a separate authorisation is required. This should be done in advance of any tasking and details of such referrals must be recorded.

18.30 CHIS RECORD KEEPING

18.31 The records relating to the source maintained by the Council will always contain particulars as laid down by the Covert Human Intelligence Sources codes of practice, revised CHIS codes of practice and the RIPA (Source Records) Regulations 2000; SI No: 2725 which details the particulars that must be included in these records.

18.32 COVERT HUMAN INTELLIGENCE SOURCES (CRIMINAL CONDUCT) ACT 2021

18.33 The Act makes provision for the use of undercover law enforcement agents and covert sources and the committing of crimes in the undertaking of their duty.

18.34 The Council is not a body designated as one that may use undercover agents and as such the Act is not applicable.

19. NECESSITY

19.1 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.

19.2 RIPA first requires that the person granting an authorisation believe that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds applicable to the Council.

19.3 The applicant must be able to demonstrate why it is necessary to carry out the covert activity to achieve the objectives and that there was no other means of obtaining the same information in a less intrusive method. The applicant must detail the crime being investigated and the information or evidence they are hoping to obtain. They should also state that they have considered other means of obtaining this information and have either concluded this is the only method available or that other methods are not appropriate and state the reason; for example it would alert the subject to their investigation which would be detrimental to the case.

20. PROPORTIONALITY

20.1 If the activities are deemed necessary, the AO must also believe that they are proportionate to the objective they are aiming to achieve. 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.

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

20.3 When completing the authorisation the AO should explain why the methods and tactics to be adopted during the surveillance are justified in the particular circumstances of the case.

20.4 The Codes provide guidance relating to proportionality which should be considered by both applicants and AOs:

- 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;
- Evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented.

20.5 When completing an application for authorisation, the case should be presented 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 authorisation.

21. COLLATERAL INTRUSION

21.1 Before authorising applications for directed surveillance, the AO should also take into account the risk of collateral intrusion - obtaining private information about persons who are not subjects of the surveillance.

21.2 Officers 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. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided this intrusion is considered proportionate to the aims of the operation. The same proportionality tests apply to anticipated collateral intrusion as to intrusion into the privacy of the intended subject of the surveillance.

21.3 All applications must include an assessment of the risk of collateral intrusion and details of any measures taken to limit this (within the relevant section of the form), to enable the AO to fully consider the proportionality of the proposed actions.

21.4 In order to give proper consideration to collateral intrusion, an AO should be given full information regarding the potential scope of the anticipated surveillance, including the likelihood that any equipment or software 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 should be made aware of its potential extent and limitations. Material which is not necessary or proportionate to the aims of the operation or investigation should be discarded or securely retained separately where it may be required for future evidential purposes. The AO should ensure appropriate safeguards for the handling, retention or destruction of such material, as well as compliance with Data Protection Act requirements.

21.5 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 should not be considered as collateral intrusion but rather as intended intrusion.

21.6 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 authority 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 should be considered, particularly (though not exclusively) where it is intended to monitor the account going forward.

22. THE APPLICATION AND AUTHORISATION PROCESS

22.1 All forms relating to RIPA can be found at https://www.gov.uk/government/collections/ripa-forms--2

22.2 DURATION OF AUTHORISATIONS

22.3 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. Authorisations should not be allowed to simply 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 Magistrate unless renewed or cancelled. Durations 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

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

22.5 APPLICATIONS/AUTHORISATION

22.6 The applicant must carry out a feasibility study and intrusion assessment as this may be required by the AO. The person seeking the authorisation should then complete the application form having regard to the guidance given in this Policy and the statutory Codes of Practice. There should not be any real delay between the feasibility study and the completion of the application form to ensure that the details within the application remain accurate. The form should then be submitted to the AO for authorisation.

22.7 When completing an application, the applicant must ensure that the case for the authorisation is presented 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.

22.8 For directed surveillance, the offence must be a criminal offence that attracts a maximum custodial sentence of six months or more or criminal offences relating to the underage sale of alcohol or tobacco under sections 146, 147 or 147A of the Licensing Act 2003 or section 7 of the Children and Young Persons Act 1933.

22.9 All the relevant sections must be completed with enough information to ensure that applications are sufficiently detailed for the AO to consider necessity and proportionality, having taken into account the collateral intrusion issues. AOs should refuse to authorise applications that are not to the required standard and should refer them back to the originating Officers. Cutting and pasting or using template entries should not take place as this would leave the process open to challenge.

22.10 If it is intended to undertake both directed surveillance and the use of a CHIS on the same surveillance subject, the respective application form and procedures should be followed, and both activities should be considered separately on their own merits.

22.11 All applications will be submitted to the AO via the Line Manager of the appropriate enforcement team in order that they are aware of the application and activities being undertaken by their staff. The Line Manager will perform an initial quality check of the application. However, they should not be involved in the sanctioning of the authorisation.

22.12 Applications, whether authorised or refused, will be issued with a unique number (obtained from the RIPA Coordinator) by the AO, taken from the next available number in the central record of authorisations which is held by the RIPA Coordinator.

22.13 If not authorised, feedback will be provided to the applicant and the application will be forwarded to the RIPA Coordinator for recording and filing.

22.14 If authorised, the applicant will then complete the relevant section of the judicial application/order form. Although this form requires the applicant to provide a brief summary of the circumstances of the case, this is supplementary and does not replace the need to supply the original RIPA authorisation form to the Court.

22.15 ARRANGING THE COURT HEARING

22.16 Within office hours a hearing must be arranged at the Magistrates' Court with Her Majesty's Courts and Tribunals Service (HMCTS). The hearing will be in private and heard by a single JP. The application to the JP will be on oath.

22.17 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. The legal department can advise who is duly authorised and able to present.

22.18 ATTENDING THE HEARING

22.19 The applicant and the AO should attend the Hearing to answer any questions directed at them. Upon attending the hearing, the presenting Officer must provide to the JP the partially completed judicial application/order form, a copy of the RIPA application/authorisation form, and the original form, together with any supporting documents setting out the case.

22.20 The original RIPA authorisation should 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.

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

22.22 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 or gave the notice was an appropriate Designated Person within the Council and the authorisation was made in accordance with any applicable legal restrictions, for example that the crime threshold for directed surveillance has been met.

22.23 DECISION OF THE JP

22.24 The JP has a number of options:

22.25 Approve or renew an authorisation. If approved by the JP, the date of the approval becomes the commencement date and the three months duration will commence on this date, the Officers are now allowed to undertake the activity.

22.26 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.

22.27 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. For example, if there was information to support the application which was available to the Council, but not included in the papers provided at the hearing.

22.28 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.

22.29 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 the Legal Department who will consider whether to make any representations.

22.30 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.

22.31 The Council may only appeal a JP decision on a point of law by judicial review. If such a concern arises, the Legal Department will decide what action if any should be taken.

22.32 POST COURT PROCEDURE

22.33 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 should be forwarded to the RIPA Coordinator. A copy will be retained by the applicant and if necessary by the AO. The Central Register of Authorisations will be updated with the relevant information to comply with the Codes of Practice and the original documents filed and stored securely.

22.34 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 of Practice.

22.35 MANAGEMENT OF THE ACTIVITY

22.36 All RIPA activity will need to be managed by all the persons involved in the process. It is important that all those involved in undertaking directed surveillance activities are fully aware of the extent and limits of the authorisation. There should be an ongoing assessment of the need for the continued activity, including ongoing assessments of the intrusion. All material obtained including evidence should be stored in line with relevant legislation and procedures to safeguard its integrity and reduce a risk of challenge. (See use of material as evidence**)**

22.37 REVIEWS

22.38 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.

22.39 In each case the AO should determine at the outset how often a review should take place. This should be as frequently as is considered necessary and practicable. Particular attention is drawn to the need to review authorisations frequently where the surveillance provides a high level of intrusion into private life or significant collateral intrusion, or may obtain confidential information. Review periods will be recorded on the application form and the decision will be based on the circumstances of each application. However, reviews should be conducted at least monthly to ensure that the activity is managed. It will be important for the AO to be aware of when reviews are required following an authorisation, to ensure timely submission of the review form.

22.40 Applicants are responsible for submitting a review form by the date set by the AO. They should also use a review form for any changes in circumstances to the original application which would comprise a change to the level of intrusion so that the requirement to continue the activity can be reassessed. The applicant does not have to wait until the review date if it is being submitted for a change in circumstances. If the circumstances or the objectives have changed considerably, or the techniques to be used are now different, a new RIPA application form should be submitted and the process followed to obtain approval by a JP.

22.41 Line managers should also make themselves aware of the required review periods to ensure that the relevant forms are completed on time.

22.42 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.

22.43 The results of a review should be recorded on the Central Record of Authorisations.

22.44 RENEWAL

22.45 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.

22.46 Renewals must be approved by a JP.

22.47 Applications for renewals should not be made until shortly before the original authorisation period is due to expire but the applicant 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).

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

22.49 AOs should examine the circumstances with regard to necessity, proportionality and the collateral intrusion issues before making a decision to renew the activity. A CHIS application should 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.

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

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

22.52 CANCELLATION

22.53 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.

22.54 As soon as the decision is taken that directed surveillance should be discontinued, the applicant or other IO involved in the investigation should inform the AO. The

AO will formally instruct the IO 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 should also be recorded in the Central Record of Authorisations**.**

22.55 The IO submitting the cancellation should complete in detail the relevant sections of the form and include the period of surveillance and also detail if any images were obtained, particularly any images containing third parties. The AO should then take this into account and issue instructions regarding the management and disposal of the images. See section below; Safeguarding and the Use of Surveillance Material.

22.56 The cancellation process should also be used to evaluate whether the objectives have been achieved and whether the applicant acted within the authorisation. This check will form part of the oversight function. Where issues are identified, they will be brought to the attention of the Line Manager and the SRO.

22.57 When cancelling a CHIS authorisation an assessment of the welfare and safety of the source should be assessed, and any issues identified and reported as above.

23. SURVEILLANCE OUTSIDE OF RIPA

23.1 As previously detailed, amendments to the Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 mean that Councils can now only grant an authorisation under RIPA where the Council is investigating criminal offences which attract a maximum custodial sentence of at least six months or criminal offences relating to the underage sale of alcohol or tobacco.

23.2 As a result of the changes in legislation, it is envisaged that surveillance may be required which falls outside of RIPA (for example in the case of anti-social behaviour disorders which do not attract a maximum custodial sentence of at least six months imprisonment).

23.3 As stated, conducting surveillance outside of RIPA is not fundamentally unlawful, however in order for the Council to defend claims that they have breached an individual's right to privacy under the HRA the Council needs to demonstrate that their actions were justified in the circumstances of the case. It is therefore the Council's policy that, in order to undertake surveillance that falls outside of RIPA, Officers will follow the same initial process as when they are making an application for authorisation under RIPA. The IO must complete a Non-RIPA application form that is authorised by an AO and the application will be lodged with and monitored by the RIPA Coordinator. The AO will need to be satisfied that the actions are necessary and proportionate and give due consideration to any collateral intrusion. The Non-RIPA authorisation form is available from the RIPA Coordinator. The procedure for review and renewal of the surveillance application will be the same, however there is no requirement/ability to obtain authorisation from a JP.

23.4 Non-RIPA surveillance also includes staff surveillance in serious disciplinary investigations. Any surveillance of staff must be formally recorded on the Non-RIPA surveillance application form and authorised by the AO in consultation with the RIPA Coordinator. The review of staff usage of the internet and e-mail would also not fall under RIPA. This surveillance outside of RIPA must however be compliant with any Council Policies with regard to monitoring at work and business practices legislation and should also consider ICO guidance in relation to surveillance of staff. Surveillance of staff should only be carried out in exceptional circumstances.

23.5 The RIPA codes also provide guidance that authorisation under RIPA is not required for the following types of activity:

- 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 Automatic Number Plate Recognition 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 criminal offence which carries a maximum sentence of 6 months imprisonment and does not relate to the sale of alcohol or tobacco to children (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.

24. SAFEGUARDING AND THE USE OF SURVEILLANCE MATERIAL

24.1 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 legally privileged information.

24.2 AUTHORISED PURPOSE

24.3 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes (for CHIS activity, this is 5 years and for surveillance activity, this is 3 years). For the purposes of the Code this is defined as follows:-

- It is, or is likely to become, necessary for any of the statutory purposes set out in the RIPA in relation to covert surveillance or CHIS activity;
- It is necessary for facilitating the carrying out of the functions of public authorities under RIPA;
- It is necessary for facilitating the carrying out of any functions of the Commissioner or the Investigatory Powers Tribunal;
- It is necessary for the purposes of legal proceedings; or
- It is necessary for the performance of the functions of any person by or under any enactment.

24.1 USE OF MATERIAL AS EVIDENCE

24.2 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 1984 and the Human Rights Act 1998.

24.3 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.

24.4 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should 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 solicitor.

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

24.6 HANDLING AND RETENTION OF MATERIAL

24.7 All material associated and obtained with an application will be subject to the provisions of all data protection legislation and regulations and CPIA Codes of Practice and to any Council Policies with regard to data retention and security. All Officers involved within this process should make themselves aware of the provisions within this legislation and how it impacts on the RIPA process. Material obtained together with relevant associated paperwork should be held securely. Extra care needs to be taken if the application and material relates to a CHIS.

24.8 Material required to be retained under CPIA should 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.

24.9 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.

24.10 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.

24.11 If an appeal against conviction is in progress when the convicted person is 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.

24.12 Retention beyond these periods must be justified under data protection legislation and regulations. AOs, through the Council's Data Controller, must ensure compliance with the appropriate Data Protection requirements and any relevant internal arrangements produced by the Council relating to the handling and storage of material.

24.13 DISSEMINATION OF INFORMATION

24.14 It may be necessary to disseminate material acquired through the RIPA covert activity within the Council or 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, should be limited to the minimum necessary. It must also be in connection with an authorised purpose as set out 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.

24.15 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.

24.16 A record will be maintained justifying any dissemination of material. If in doubt, seek legal advice.

24.17 STORAGE

24.18 Material obtained through covert surveillance, 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 (where applicable). This requirement applies to all those who are responsible for the handling of the material. It will be necessary to ensure that an appropriate security clearance regime is in place to safeguard the material whether held electronically or physically.

24.19 COPYING

24.20 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.

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

24.22 DESTRUCTION

24.23 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.

25. ERRORS

25.1 Proper application of the surveillance provisions in the RIPA codes and this Policy should reduce the scope for making errors.

25.2 RELEVANT ERROR

25.3 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 would include compliance by public authorities with Part II of RIPA.

25.4 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 of Practice relating to the safeguards of the material.

25.5 Errors can have very significant consequences on an affected individual's rights. All relevant errors made by the Council must be reported to the Investigatory Powers Commissioner as soon as reasonably practicable, and a full report no later than ten working days after the error is discovered. 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.

25.6 SERIOUS ERRORS

25.7 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.

25.8 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.

26. COMPLAINTS

26.1 The Investigatory Powers Tribunal (IPT) has jurisdiction to investigate and determine complaints against the Council's use of investigatory powers, including those covered by this code. Any complaints about the use of powers as described in this code should be directed to the IPT.

26.2 Complaints should be addressed to:
The Investigatory Powers Tribunal
PO Box 33220
London, SWIH 9ZQ

27. STRATEGY AND POLICY REVIEW

27.1 The Counter Fraud Unit will review and amend this Policy as necessary to ensure that it continues to remain compliant and meets legislative requirements and the vision of the Council.

Responsible Department: Counter Fraud Unit

Review frequency as required by legislative changes / every year.