AUDIT AND GOVERNANCE COMMITTEE

29 September 2026

EXECUTIVE HEAD OF GOVERNANCE AND LAW
REPORT NO. LEG2603

CORPORATE POLICY AND GUIDANCE ON SURVEILLANCE AND THE USE OF THE REGULATION OF INVESTIGATORY POWERS ACT 2000

SUMMARY AND RECOMMENDATION:

SUMMARY:
To update Members of the Council's surveillance activities within and outside the scope of the Regulation of Investigatory Powers Act 2000 (RIPA).

RECOMMENDATION: To note the contents of this report.

1. INTRODUCTION

1.1 Most of the surveillance carried out by the Council will be done overtly, that is, that officers will be going about Council business openly.

1.2 The Council's corporate policy on the use of covert techniques under RIPA should be reviewed on a regular basis. The powers under RIPA are used infrequently, if at all some years.

1.3 The Investigatory Powers Commissioner's Office (IPCO) reviews Rushmoor Borough Council's policies and procedures relating to RIPA on a regular basis.

1.4 Most of the surveillance undertaken by the Council is outside of RIPA, for example, for planning enforcement purposes or under Licensing legislation. The IPCO have made clear in their guidance that robust processes and procedures need to be in place for any surveillance carried out, whether under the RIPA provisions or under separate legislation.

1.5 CCTV surveillance across the Borough is carried out by Runnymede Borough Council, on behalf of Rushmoor Borough Council, with the appropriate General Data Protection Regulation (GDPR) and contractual arrangements in place. The CCTV surveillance is outside of RIPA.

2. BACKGROUND

2.1 Council officers who carry out investigations as part of their duties sometimes need to consider using covert techniques, i.e., techniques that leave the subject of the investigation unaware that they are being observed or investigated.

2.2 RIPA provides a framework within which such techniques may be used. All RIPA authorisations must now be approved by the Magistrates' Court before any surveillance can take place.

2.3 It should be noted that surveillance outside of RIPA will be undertaken and it is important that this is lawful and takes account of human rights legislation.

2.4 Only trained and authorised Council officers may authorise and undertake covert surveillance, all of which is subject to detailed scrutiny by the Investigatory Powers Commissioner's Office (IPCO).

2.5 In March 2026, comprehensive training was provided to staff who are involved in surveillance activities.

3. UPDATE

3.1 There have been no requests for RIPA authorisation via Legal Services, since the last report in September 2025.

3.2 In April 2026, the Council completed a self-assessment of its RIPA activities at the request of the Investigatory Powers Commissioner's Office (IPCO).

3.3 On 13 April 2026, the IPCO confirmed that it was satisfied with the Council's self-assessment response which provided assurance that ongoing compliance with RIPA 2000 and the Investigatory Powers Act 2016 will be maintained. The IPCO confirmed it was content with the Council's RIPA policies and related governance in place and requested that the Council continue with ongoing training and awareness raising; internal compliance monitoring by lead Managers within their service areas; and the retention, review and destruction of any product obtained through the use of covert powers.

3.4 A further inspection by the IPCO is not expected until 2029 and the IPCO have been informed that by the time the next inspection is due to take place, this Council will have dissolved and will be part of a new unitary Council. In light of the government announcement relating to Local Government Reorganisation, once clarity is received from MHCLG, IPCO will be updated if necessary.

3.5 Over recent months, Legal Services have undertaken a comprehensive review of the Council's Surveillance and RIPA Policy and Guidance. The review has informed the drafting of a new Surveillance and RIPA & Investigatory Powers Act 2016 (IPA) as Amended by Investigatory Powers (Amendment) Act 2024 Policy and Guidance, which is currently being finalised to ensure it remains accurate and up to date. A new Surveillance and RIPA & IPA Policy and Guidance incorporates all relevant updates to the RIPA & IPA Statutory framework namely:

i) CHIS Revised Code of Practice December 2022
ii) Covert Surveillance and Property Interference Revised Code of Practice February 2024
iii) Investigatory Powers (Amendment) Act 2024
iv) Communications Data Code of Practice June 2025

4. LEGAL IMPLICATIONS

4.1 A review of the Council's Surveillance and RIPA Policy and Guidance on the use of surveillance and use of powers under RIPA and IPA is required to ensure that it complies with any changes in the law.

5. FINANCIAL AND RESOURCE IMPLICATIONS

5.1 There are no additional financial implications.

6. EQUALITIES IMPACT IMPLICATIONS

6.1 No equalities issues arise, however before undertaking any covert surveillance an equalities impact assessment should be undertaken.

7. SUMMARY

7.1 No covert surveillance has been undertaken by the Council this year.

7.2 In April 2026, the Investigatory Powers Commissioner's Office confirmed that it was content with the Council's policies and RIPA activities.

7.3 A new Draft Surveillance and RIPA & IPA Policy and Guidance is submitted in conjunction with this Report for review by the Audit & Governance Committee for approval.

RECOMMENDATION: That the Audit and Governance Committee approve the Surveillance and RIPA & IPA Policy and Guidance at Appendix 1 to this report.

CONTACT DETAILS:

Report Author
Amanda Bancroft – Executive Head of Governance and Law (Monitoring Officer)
amanda.bancroft@rushmoor.gov.uk

Surveillance and Regulation of Investigatory Power Act 2000 (RIPA) & Investigatory Powers Act 2016 (IPA) as Amended by Investigatory Powers (Amendment) Act 2024

Policy and Guidance

__________ 202__

RUSHMOOR BOROUGH COUNCIL

Table of Contents

LIST OF ACRONYMS

ACRONYM	MEANING
RIPA	Regulation of Investigatory Powers Act 2000
IPA	Investigatory Powers Act 2016
IPCO	Investigatory Powers Commissioner’s Office
NAFN	National Anti-Fraud Network
OCDA	Office for Communications Data Authorisations
JA	Judicial Approval
SRO	Senior Responsible Officer
AO	RIPA Authorising Officer
DSO	CD Designated Senior Officer
SPOC	Single Point of Contact
URN	Unique Reference Number
DS	Directed Surveillance
CHIS	Covert Human Intelligence Source
IS	Intrusive Surveillance
CD	Communications Data
CRR	Centrally Retrievable Record
DO	Disclosure Officer

PART A: RIPA 2000, Surveillance and Human Intelligence Sources

1. Introduction and Key Measures

1.1 Introduction

1.1.1 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 and as such, should not be undertaken without full and proper consideration.

1.1.2 The Human Rights Act 1998 (HRA) gave effect in UK law to the rights of individuals enshrined in the European Convention on Human Rights 1950 (ECHR). All surveillance activity can pose a risk to the Council from challenges under the Human Rights Act 1998 or other processes. Therefore, it must be stressed that all staff involved in the process must take their responsibilities seriously which will assist with the integrity of the Council's processes, procedures and oversight responsibilities.

1.1.3 When public authorities seek to obtain private information through covert surveillance, Article 8 of ECHR - which protects an individual's right to respect their private and family life, home, and correspondence - is the provision most likely to be engaged.

1.1.4 Regulation of Investigations Powers Act 2000 (RIPA) provides the statutory framework to enable covert surveillance to be lawfully authorised and conducted and the Investigatory Powers Act 2016 (IPA) provides the statutory framework for the acquisition of Communications Data (CD) whilst ensuring the public authority does not infringe a person’s Article 8 rights, except as may be permitted by Article 8(2). Consequently, a public authority can act in a way that is compatible with the ECHR and HRA.

1.1.5 If having read this document you are unclear about any aspect of the process, seek advice from Legal Services.

1.2 Purpose and Objectives

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

1.2.2 This document provides guidance on the authorisation processes and the roles of the respective staff involved.

1.2.3 The Senior Responsible Officer (SRO) is duly authorised by the Council to monitor, review, and amend this Policy as and when required. **Appendix 1** sets out the designation of the Senior Responsible Officer. For administration and operational effectiveness, the SRO is also authorised to add or substitute an Authorising Officer or Designated Senior Officer when required.

1.2.4 The policy also provides guidance on surveillance which is necessary to be undertaken by the authority but cannot be authorised under the RIPA legislation. This type of surveillance will have to be compliant with the Human Rights Act.

1.2.5 The policy also identifies the cross over with other policies and legislation, particularly with the Data Protection Act and the Criminal Procedures Act.

1.2.6 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 for both Directed Surveillance and the use of Covert Human Intelligence Sources (CHIS). The Codes of Practice are available from:

1.2.7 Covert surveillance code of practice - GOV.UK - current version issued in February 2024

1.2.8 Covert Human Intelligence Sources code of practice 2022 - GOV.UK - current version issued in December 2022.

1.3 Background to RIPA and Lawful Criteria

1.3.1 On 2nd October 2000 the Human Rights Act 1998 (HRA) came into force, making it potentially unlawful for a Local Authority to breach any article of the ECHR.

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

1.3.2.1 Everyone has respect for his private and family life, his home and his correspondence.

1.3.2.2 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.

1.3.3 The right under Article 8 is a qualified right and Public Authorities can interfere with this right for the reasons given in 4.2 (2) above if it is necessary and proportionate to do so.

1.3.4 Those who undertake Directed Surveillance or CHIS activity on behalf of a Local Authority may 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.

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

1.3.6 However, under RIPA, Local Authorities can now only authorise Directed Surveillance for the purpose of preventing or detecting conduct which constitutes a criminal offence which is punishable (whether on summary conviction or indictment) by a maximum term of at least six months imprisonment; (serious crime criteria) or involves the sale of alcohol or tobacco to children.

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

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

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

1.4 Legal implications

1.4.1 Although the lack of authorisation does not automatically make surveillance activity unlawful, it may result in significant legal and procedural consequences:

1.4.1.1 Evidential Impact: Any evidence obtained may be deemed inadmissible in court proceedings.

1.4.1.2 Human Rights Claims: Individuals subject to surveillance may pursue claims under Article 8 of the Human Rights Act, alleging an infringement of their right to privacy.

1.4.1.3 Reputational and Financial Risk: A successful Article 8 challenge could result in reputational damage to the Council and potential liability for financial compensation.

1.4.1.4 Tribunal Complaints: The Government has established the Investigatory Powers Tribunal (IPT), which allows individuals to lodge complaints if they believe their rights have been breached.

1.4.1.5 Regulatory Reporting: The activity may be classified as an error, requiring investigation and a formal report by the Senior Responsible Officer to the Investigatory Powers Commissioner's Office (IPCO).

1.5 Financial Implications

1.5.1 Failure to obtain proper authorisation may result in indirect costs such as legal challenges, reputational damage, and potential compensation claims.

1.6 Impact assessment (IA) record

Data Protection IA required?	(No)
Equalities IA required?	(Yes)
Climate Change IA required?	(No)

2. Surveillance

2.1 Surveillance for the purposes of RIPA includes:

2.1.1 monitoring, observing, or listening to persons, their movements, their conversations or their other activities or communications;

2.1.2 recording anything monitored, observed, or listened to in the course of surveillance;

2.1.3 surveillance by or with the assistance of a surveillance device.

2.2 Scope of Surveillance

2.2.1 Surveillance may be conducted with or without the assistance of a surveillance device, includes the recording of any information obtained and can be undertaken whilst on foot, mobile or static. Surveillance also includes references to the interception of a communication in the course of its transmission by means of a postal service of telecommunication system, if and only if the communication is sent by, or intended for, a person who has consent to the interception of their communications, and there is no separate warrant authorising that interception.

2.3 Methods of recording

2.3.1 Methods of "recording," surveillance were expanded by the Protection of Freedoms Act 2012, which dealt with the regulation of CCTV and other surveillance camera technology and introduced the Surveillance Camera Code of Practice. The Act states "surveillance camera systems include… any other systems for recording or viewing visual images for surveillance purposes" which includes Body Worn Videos.

2.4 Lawful Surveillance

2.4.1 Surveillance will be lawful if an authorization confers an entitlement to engage in that conduct on the person whose conduct it is and his conduct is in accordance with an authorisation.

2.5 Types of Surveillance

There are two types of surveillance, namely overt and covert.

2.5.1 **Overt Surveillance**. Most surveillance carried out by the Council will be overt, thus it will fall outside the remit of RIPA. An example of overt surveillance is the Council's overt CCTV.

2.5.2 **Covert Surveillance**. Surveillance is covert if and only if, it is carried out in a manner that is calculated to ensure that persons who are the subject to the surveillance are unaware that it is or may be taking place.

2.5.3 **Categories of Covert Surveillance**. There are three categories of covert surveillance:

(i) Directed
(ii) Covert Human Intelligence Source (CHIS)
(iii)**Intrusive**. Please note, local authorities are prohibited from conducting intrusive surveillance.

2.5.4 **Directed Surveillance**. Directed surveillance (DS) is covert but not intrusive surveillance which is undertaken:

(i) for the purposes of a specific investigation or a specific operation;
(ii) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
(iii)is conducted otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought for the carrying out of the surveillance.

2.5.4.1 Example. An Investigation into a suspect (target) who claimed Direct Payment from a Council based upon his declared disabilities. It is suspected the target is not disabled, partially sighted and/or has substantially exaggerated his injuries. Officers wish to undertake a covert DS operation involving officers positioned in an unmarked van outside of the target's home address. The intended directed surveillance operation intends to capture by photographs and video, the target attending and/or exiting the property, to ascertain his method of transport, whether he is the driver or passenger and the extent to which he can walk unaided.

2.5.4.2 The proposed DS operation is covert, is to be used for a specific investigation and will be conducted in a manner likely to result in obtaining private information about the target, namely his movements, mobility, family members and his daily activities in and around his home address. Accordingly, the intended surveillance operation constitutes DS, therefore a RIPA DS authorisation and Judicial Approval is required.

2.5.5 **Covert Human Intelligence Sources (CHIS)**. A CHIS is perhaps more commonly known as an informant.

2.5.5.1 A person is a CHIS if they/them:

(a) establish or maintain a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paragraphs (b) or (c);
(b) covertly uses such a relationship to obtain information or provide access to any information to another person; or
(c) covertly discloses information obtained by the use of such a relationship, or as a consequence of the existence of such a relationship.

2.5.5.2 A relationship is established or maintained for a covert purpose if any 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. A covert relationship and information obtained from it is disclosed covertly, if and only if it is to be used, or as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question.

2.5.5.3 Most CHIS applications are for both use and conduct of a CHIS as the CHIS is usually tasked to undertake covert action and once completed to respond to tasking. Care should be taken to ensure the CHIS is clearly instructed on the type and remit of the task and that all CHIS activities are properly risk-assigned.

2.5.5.4 In practice the reactive nature of the work of a CHIS and the need for a CHIS to maintain cover may make it necessary to engage in conduct which was not envisaged at the time the authorisation and Judicial Approval was granted. Such conduct is deemed incidental and is regarded as property authorised even if not included in the initial authorisation but is likely to occur only in exceptional circumstances.

2.5.6 Key Difference Between Directed Surveillance (DS) & CHIS

The key difference is that DS involves obtaining private information through covert means, whereas a CHIS involves the manipulation of a relationship to obtain information.

2.5.7 Establishing, Maintaining & Using a Relationship

Establishing a relationship means the "set up," and maintenance of the relationship but which does not require endurance over any particular period e.g. a relationship of seller and buyer may be deemed to exist between a shopkeeper and customer even if only a single transaction takes place. Repetition of a sale does not determine the existence of a relationship as this is determined on all the circumstances including the length of time of the contact between the two and the nature of any covert activity.

<u>Example 1</u>
Intelligence suggests a local shopkeeper openly sells alcohol to underage customers without asking any questions. The Council task a trained juvenile to make a purchase of alcohol where no prior discussion between the shopkeeper and juvenile is required and thus it is not necessary to establish a relationship between the two. The tasked juvenile is not a CHIS, but it is good practice to obtain a Directed Surveillance Authorisation.

<u>Example 2</u>
A like scenario but where the shopkeeper only sells to juveniles known to and trusted by them from a room at the back of the shop. To gain access to the room it is necessary for the trained tasked juvenile to first be deployed to establish a relationship between the two so that he can gain the shopkeeper's trust. In these circumstances a relationship was necessary and so was established and maintained for a covert purpose, thus a CHIS authorisation is required

2.5.8 A CHIS may be an officer or member of the public.

2.5.9 Relevant Source

This is a CHIS who holds an office, rank or position with the public authority. Local authorities are prohibited from using this type of CHIS.

2.5.10 Participating CHIS's

This type of CHIS is specifically authorised to participate in criminal conduct. Local authorities are prohibited from using this type of CHIS.

2.5.11 Online Role Player

2.5.11.1 Suspects' increased use of social media has led to CHIS techniques expanding to include the use of online CHISs, known as a "role players" who do not disclose their true identity. Any covert online operation that meets the definition set out in paragraph 2.5.5.1 constitutes the use of a CHIS, even where the relationship exists solely in an online environment.

2.5.11.2 The fora in which online role players can be deployed in include social media sites, chatrooms and online gaming apps. In some scenarios the amount of interaction required will not be sufficient to establish a relationship, so the role player will not be a CHIS but will still require a DS authorisation if the other criteria are met. E.g. sending or receiving a friend request, liking a post, or even entering a closed group known to be administered by a subject of interest. By contrast, if once in that closed group, the officer seeks to obtain information by establishing a relationship with a member, they are a CHIS.

2.5.11.3 Where the use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with the CHIS Revised Code December 2022, should include consideration of the risks arising from that online activity, including factors such as the length of time spent online and the material to which the CHIS may be exposed. This should also take into account of any disparity between the technical skills of the CHIS and those of the handler or AO and the extent to which this may impact on the effectiveness of oversight.

2.5.11.4 Where it is intended that one or more officer shares the same online persona, each officer should be clearly identifiable within the overarching authorisation for that operation. The authorisations should provide clear information about the conduct required of each officer and including risk assessments in relation to each officer involved.

2.5.12 Test Purchasing

The Council's position regarding test purchases for one-off sales carried out by either an adult or juvenile is that such conduct does not constitute CHIS, as the purchaser is not required to, nor does he/she establish any relationship in a one-off sale. However, you should consider whether test purchasing requires a DS authorisation, particularly where it is intended to covertly record the test purchase.

2.5.13 Public Volunteer

2.5.13.1 In many cases involving human sources, a relationship will not have been established or maintained for a covert purpose. Members of the public often volunteer or provide information which they have observed or acquired other than through a relationship and without having been induced, asked, or tasked which is not a CHIS scenario. Even if the volunteer was subsequently tasked to continue to obtain and provide such information to the Council if it is not necessary to establish or maintain a relationship in order to obtain and provide this information the informant does not become a CHIS, although it would require a DS authorisation.

2.5.13.2 A resident contacts Rushmoor Borough Council to report suspected drug dealing in a council-owned car park in Farnborough, based on what they have casually observed while parking their own vehicle.

The resident is not a CHIS at this point, as the information is volunteered and not obtained through a relationship established or maintained for a covert purpose. However, if council officers later ask the resident to keep watch on specific individuals, note vehicle registration numbers, or report patterns of activity during particular times, and the resident agrees to do so, the resident would then be tasked to obtain further information. At that point, a CHIS authorisation would be required. This change in role constitutes "status drift".

2.5.14 Use of Equipment by a CHIS

A CHIS wearing or carrying a surveillance device does not need a separate directed or intrusive surveillance authorisation provided the device will only be used in the presence of the CHIS. Please note, local authorities are prohibited from carrying out Intrusive Surveillance.

2.5.15 Local Considerations & Community Impact Assessments

For CHIS applications the Applicant, AO and Magistrate need to be aware of any sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of the CHIS. Consideration should also be given to any adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from that CHIS. The Code recommends that where an AO considers that conflicts may arise, they should consult a senior officer within the police force areas in which the CHIS is deployed. All public authorities should also consider consulting with other relevant public authorities to gauge community impact.

2.6 Special Considerations for CHIS Authorisations

For both vulnerable individuals and juveniles, only the Head of Paid Service or the person acting as Head of Paid Service are permitted to authorise CHIS Applications and/or Renewals. Further, the Investigatory Powers Commissioner's Office must be informed within 7 days of a CHIS authorisation of a vulnerable adult or a juvenile source.

2.6.1 Vulnerable Individuals

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 themselves, or unable to protect themselves against significant harm or exploitation. A vulnerable individual should only be authorised to act as a CHIS in the most exceptional circumstances.

2.6.2 Juveniles

Whilst it is unlikely the Council will deploy a juvenile CHIS, if utilised, the following enhanced safeguards for Juvenile CHIS's (under 18) must be complied with:

(a) Juvenile CHIS only authorised in exceptional circumstances and subject to enhanced risk assessment process for which where appropriate, external advice should be sought;
(b) CHIS under 16 must not be authorised to give information against their parents or person with parental responsibility for them;
(c) Juvenile CHIS Authorisation duration 4 months;
(d) Separation between those responsible for the investigation and those authorising and managing CHIS;
(e) Appropriate adult normally parent or guardian unless unavailable or specific reasons to exclude them;

In addition to the requirements and safeguards of RIPA, the Orders and Code of Practice, relevant public authorities may also wish to put in place further internal guidance to support their staff in the operation of a CHIS, for example a process to be followed as to how to safeguard and promote the wellbeing of the juvenile CHIS, including how to assess their maturity and capacity to give informed consent; a requirement to ensure the handlers are property trained to deal with young people and requirements to consider all aspects of safeguarding to a young person.

2.7 Management of a CHIS

2.7.1 Tasking is the assignment given to the CHIS asking them to obtain, provide access to or disclose information. In order, for an Authorising Officer ("AO") to be able to grant a CHIS authorisation, both the AO and Magistrate, must believe that in addition to the operation being necessary and proportionate, arrangements exist ensuring:

(a) there will be at all times a "handler," of the specified rank with the relevant investigatory authority, with day-to-day responsibility for the source." The handler is responsible for dealing with the CHIS; directing day to day activities; recording the information supplied by the CHIS and monitoring the CHIS's security and welfare.

(b) that there will be at all times a "controller," of the specified rank with the relevant investigatory authority with general oversight of the use made of the source, responsible for the management and supervision of the handler and general oversight of the us of this CHIS.

2.8 CHIS Records

Detailed records must be kept of the authorisation and use made of a CHIS. In addition, records of copies of the following should be kept for at least six years:

(a) a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
(b) a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;

(c) the reason why the person renewing an authorisation considered it necessary to do so;
(d) any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
(e) any risk assessment made in relation to the CHIS;
(f) the circumstances in which tasks were given to the CHIS;
(g) the value of the CHIS to the investigating authority;
(h) a record of the results of any reviews of the authorisation;
(i) the reasons, if any, for not renewing an authorisation;
(j) the reasons for cancelling an authorisation; and
(k) the date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease.

2.9 Security & Welfare

Any public authority deploying a CHIS should take into account the safety and welfare of the CHIS when carrying out actions in relation to an authorisations or tasking, and the foreseeable consequences to others of that tasking[11] and undertake a risk assessment before granting the authorisation. The ongoing security and welfare of the CHIS after the cancellation of the authorisation should also be considered at the outset and reviewed during the authorisation period of the CHIS.

Consideration must also be given to the management of any requirement to disclose information which could risk revealing the existence or identity of the CHIS. Strategies minimising the risks to a CHIS or others should be put in place.

2.10 Intrusive Surveillance

As set out above, local authorities are prohibited from carrying out intrusive surveillance. Intrusive surveillance involves the presence of an individual on residential premises or in a private vehicle or is carried out by means of a surveillance device. Surveillance equipment outside the premises or vehicle will not be intrusive unless the device consistently provides information of the same quality and detail as might be expected from a device that is in the premises/vehicle. DS carried out on premises ordinarily used for legal consultations at a time when they are being used as such is to be treated as intrusive surveillance.

2.11 Online Overt & Covert Surveillance including Social Media/Networking Sites

2.11.1 The Council has in place a Council Internet and Social Media Research Investigations Procedure, which specifically addresses the use of social media for investigative purposes.

2.11.2 Permitted Online Access. To undertake any form of overt and/or covert online surveillance Staff/officers must only use a social media account; account name; login details that have been authorised, created, and is controlled by an AO on behalf of the Council.

2.11.3 Officers are <u>prohibited</u> from:

2.11.3.1 using their own personal social media accounts and /or their personal login details to undertake intelligence gathering and/or any form of overt or covert surveillance;

2.11.3.2 using a false identity(pseudonym) to carry out overt surveillance;

2.11.3.3 using a false identity (pseudonym) to carry out covert surveillance unless this activity, pseudonym, and details of the true identity of the officer are all contained in the DS or CHIS application, which must be authorised by an AO and Judicial Approval granted;

2.11.3.4 adopting the identity of a person known, or likely to be known to the subject of interest and/or users of the site for either overt and/or covert DS or to be used by a CHIS;

2.11.4 Online Overt Activity. Publicly Available information (PAI)

2.11.4.1 In addition to utilising online role players as CHIS's, there is a wealth of information available online which provides opportunities to view and/or gather intelligence and/or evidence. This is often referred to as publicly available information (PAI) or open source research.

2.11.4.2 The fact content of many social media sites and websites are freely accessible requires consideration of and in accordance with RIPA. Consideration must therefore be given as to the likelihood of the subject knowing that the surveillance is or may be taking place. Where a public authority has taken reasonable steps to inform the public or particular individuals that the surveillance is or may be taking place, the activity may be regarded as overt and therefore a DS authorisation is not required. Information about an individual on a publicly accessible database such as Companies House is where the individual is unlikely to have any reasonable expectation of privacy over the monitoring by public authorities of that information, hence a DS authorisation is not required.

2.11.5 Online Covert Activity

2.11.5.1 The use of a Council controlled account(s) to undertake online covert activity to undertake initial intelligence; establish or check basic facts or carry out general observation duties including the monitoring of publicly accessible areas of the internet in circumstances where it is not part of a specific investigation or operation does not require a DS authorisation.

2.11.5.2 Where online monitoring or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group including the systematic collection and recording of information, a DS authorisation should be considered. When it is intended to engage with others online without disclosing their identity, a CHIS authorisation may be needed.

2.11.5.3 The key issue to determine if a DS authorisation is required is the intended purpose and scope the online activity is proposed to undertake.

2.11.6 Online Covert Directed Surveillance

2.11.6.1 Factors to be considered in establishing whether a DS authorisation is required for online covert directed surveillance include:

i) Whether the investigation or research is directed towards an individual or organisation;
ii) Whether it is likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.6 above);
iii) Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile;
iv) Whether the information obtained will be recorded and retained;
v) Whether the information is likely to provide an observer with a pattern of lifestyle;
vi) Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
vii) Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
viii) Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties;
ix) An example would be a local Facebook

2.11.6.2 An example would be a local Facebook buy and sell group with 5000 members. The Council is investigating a subject and it was known the subject advertised counterfeit items for sale within this Facebook group which first required the group's administrator to accept the invite request to join. If an officer sent an invite to join the group in order to identify, access and monitor the posts of the subject as part of this investigation, then despite the fact it was a large Facebook group with no privacy settings once membership was authorised, a DS authorisation should be sought as when the administrators made the group publicly available with no privacy settings, it was not anticipated that the information accessible would be used for a covert purpose such as this investigation.

2.11.7 Repeated or systematic viewing, collecting, or recording of private information from "open," social media sources such as Facebook, Snapchat, and LinkedIn including information relating to the interests, activities and movements of individuals and their associates could be regarded as covert surveillance. Once the access and study of an individual's online presence becomes persistent or where any material obtained is to be extracted and recorded and may engage privacy considerations, such as screenshotting a Facebook account, then a DS RIPA authorisation should be obtained.

2.11.8 Please note, internet searches carried out by third parties on behalf of a public authority may still require a DS authorisation.

2.11.9 Online Covert CHIS

2.11.9.1 Any member of a public authority, or person acting on their behalf, who conducts activity on the internet in such a way that they may interact with others, whether by publicly open websites such as an online news and social networking service, or more private exchanges in circumstances where the other parties could not reasonably be expected to know their true identity, they should consider whether the activity requires a CHIS authorisation.

2.11.9.2 An example would be the Council tasks an officer to covertly purchase goods from several websites to obtain information about the identity of the seller, country of origin of the goods and banking arrangements. In doing so the officer will be required to engage with the seller to obtain the information required and to complete the purchases. This scenario requires the officer to establish and maintain a relationship with the seller and therefore a CHIS authorisation is required.

2.11.9.3 This section should be read in conjunction with CHIS – Online Role Players above.

2.12 Local Authority RIPA Prohibitions

2.12.1 Local authorities are prohibited from carrying out:

i) Intrusive Surveillance;
ii) Property Interference;
iii) Authorising urgent authorisations;
iv) CHIS Criminal Conduct authorisations;

2.12.2 If any officer considers trespass is required as part of any authorised surveillance this would constitute property interference which is prohibited. The surveillance should therefore cease immediately, and the operation should be referred to both the AO and SRO as a matter of urgency

2.13 Local Authority RIPA Limitations

2.13.1 Judicial Approval of Local Authority RIPA authorisations

Authorisations and notices under RIPA for the use of directed surveillance and CHIS are not effective until Judicial Approval has been granted by a Justice of the Peace

2.14 Directed surveillance Crime Threshold Test

2.14.1 The Crime Threshold Test only applies to authorisations and renewals for Directed Surveillance. Local authorities are only permitted grant an authorisation for directed surveillance for criminal offences which either are:

i) punishable by a maximum custodial sentence of six months or more; or
ii) related to the underage sale of alcohol or tobacco; or
iii) related to underage sale and/or proxy purchasing of nicotine inhaling products

2.14.2 If an officer is unsure of the relevant criminal offence(s) being investigated or the penalties, legal advice should be obtained from Legal Services. If no offence is identified and/or the offences identified do not satisfy the Crime Threshold Test, a DS RIPA application should not be submitted and/or authorised.

2.15 Prevention of Disorder

Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless it involves a criminal offence punishable by a maximum of term of at least 6 months. Local authorities are therefore no longer permitted to use RIPA for low level offences. These restrictions therefore require consideration at the commencement of an investigation if the conduct amounts to criminal offence which would satisfy the Crime Threshold test. If during the investigation the position changes so the conduct amounts to a less serious offence not meeting the threshold, then any live directed surveillance authorisation should be cancelled forthwith.

2.16 Two Mandatory Test For Directed Surveillance & CHIS

2.16.1 Necessity

2.16.1.1 A local authority AO shall not grant an authorisation for the carrying out of Directed Surveillance and/or CHIS unless they believe the authorisation is necessary. The sole necessity ground applicable to local authorities is," for the purpose of preventing or detecting crime or disorder."

2.16.1.2 The officer completing and submitting the application must carefully explain why it is necessary to use the covert technique requested and the AO must explain why/she is satisfied the covert surveillance is necessary. Please note, in the case of Directed Surveillance the Crime Threshold Test must also be satisfied (see above).

2.16.2 Proportionality

2.16.2.1 A local authority AO shall not grant an authorisation for the carrying out of Directed Surveillance and/or CHIS unless they believe the authorised surveillance is proportionate to what is sought to be achieved by carrying it out. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

2.16.2.2 The following should be considered in determining proportionality:

i) balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or harm;
ii) explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

iii) considering whether the activity is an appropriate use of the legislation and a reasonable way, having considered all reasonable alternatives, of obtaining the information sought;
iv) evidencing, as far as reasonably practicable, what other methods had been considered and why they were not implemented, or have been implemented unsuccessfully;

2.16.2.3 The AO must consider the risk of obtaining private information about persons who are not the subjects of the surveillance (collateral intrusion) and whether the proposed activity is proportionate. The AO's considerations need to be fully documented within the RIPA Form.

3. Key Roles (RIPA – Covert Surveillance & CHIS)

3.1 Senior Responsible Officer

3.1.1 The Council's Senior Responsible Officer (SRO) is the Executive Head of Governance & Law (Monitoring Officer).

3.1.2 The Codes for Directed Surveillance, CHIS and Communications Data specify the SRO is responsible for:

3.1.2.1 The integrity of the process in place within the public authority to authorise directed surveillance and request communications data;

3.1.2.2 Compliance with RIPA, Investigatory Powers Act (IPA) and Codes of Practice

3.1.2.3 Oversight of the reporting errors to the Investigatory Powers Commissioner (IPC) and the identification of both the cause(s) of errors and implementation of processes to minimize repetition of errors;

3.1.2.4 Engagement with IPCO and inspectors who support the Commissioner when they conduct their inspections;

3.1.2.5 Where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Judicial Commissioner, similarly the Investigatory Powers Commissioner (IPC).

3.1.2.6 Ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the IPC

3.1.2.7 The SRO is responsible for and required to provide or organise training for AO's and certifying any new AO. The SRO is authorised to retract an AO's certification and authorisation if it is felt the AO has either not complied with the statutory framework and/or this Policy. To reactivate an AO's RIPA certificate of authorisation further approved training will be required. The SRO is also responsible for ensuring all relevant members of staff who do or may utilise RIPA as "Applicants," receive RIPA training including refresher training, to ensure they are aware of the RIPA statutory framework and process.

3.2 Authorising Officers

3.2.1 A designated AO is lawfully permitted to grant authorisations for Directed Surveillance or use of a CHIS and responsibility remains with the AO after Judicial Approval. AOs must also authorise reviews, renewals and cancellations. The rank of local (AO's) lawfully permitted to act as AO are Director, Head of Service, Service Manager or equivalent. The council's list of AOs is contained within the **Appendix 2**. Before and in order to become an AO, training must be completed and the SRO must authorise the AO to commence their role. Only the Head of Paid Service can authorise juvenile CHISs or vulnerable persons (see paragraph 2.6).

3.2.2 The AO must be satisfied that the proposed activity is both necessary and proportionate. AO's should routinely sate the "who, what, when and how," regarding the proposed activity. Care must also be taken to ensure the words used do not unintentionally limit the activity which can be avoided by using words such as "and/or" to permit both alternatives. AOs must also pay particular attention to Health & Safety issues that may arise or be raised by proposed surveillance and must not approve an application for either DS or CHIS unless they are satisfied that the Health & Safety risks are managed and proportionate. If any AO is in doubt, they should obtain prior guidance from a member of the Council's Health & Safety Officer and/or the SRO. All AOs should wherever possible be independent of the investigation and this is one of the criteria within the RIPA URN Request Form, a template of which is contained within the **Appendix 10**. Where the AO authorises their own activity, this will be recorded in the RIPA Centrally Retrievable Record. A template of the Record is contained within the **Appendix 5** and should be highlighted to the IPCO inspector at the next inspection.

4. RIPA Defined Terms

4.1 Private Information

4.1.1 Private information relates to a person who has or may have a reasonable expectation of privacy, including any information relating to his private or family life, such as a person's private or personal relationship with others such as family and professional or business relationships. Whilst a person may have a reduced expectation of privacy in a public place, covert surveillance of that person's activities may still result in obtaining private information.

4.2 Collateral Intrusion

4.2.1 Directed Surveillance

Collateral intrusion is the obtaining of private information about persons who are not subject of the surveillance. Measures should be taken wherever practicable to avoid or minimise unnecessary intrusion into the privacy of non-subjects. Where such collateral intrusion is unavoidable, the activities may still be authorised, provided the intrusion proportionate to what is sought to be achieved. Where the proposed surveillance is specifically against non-subjects in the overall investigation, interference with that person's privacy should not be considered as collateral intrusion but intended intrusion. Where the Council intends to access a social media or other online account to which they have been given access by consent of the owner, the applicant officer will need to consider whether the account may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, a DS Authorisation should be obtained as the third party has not consented to and is likely to be unaware of the surveillance.

4.2.2 CHIS

Before authorising the use or conduct of a CHIS, the AO should take into account the risk of interference with and wherever practicable, avoid or minimise interference with the private or family life of persons who are not the intended subjects of the CHIS activity.

4.3 Confidential Or Privileged Material

4.3.1 Particular consideration must be given in cases where the subject of the investigation/operation might reasonably assume a high degree of confidentiality. This includes material from the following categories:

(a) Confidential journalistic material or a journalist's source;
(b) Legally privileged;
(c) Confidential personal information such as medical records or communications between an MP and another person or constituency business;

4.4 Confidential Information

4.4.1 Confidential information is information held in confidence concerning an individual (living or dead) who can be identified from it and the material in question relates to their physical or mental health or spiritual counselling. Authorisations containing confidential information can only be authorised by the Chief Executive (Head of Paid Service).

4.5 Confidential Journalistic Material & Journalistic Sources

4.5.1 Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in such information being obtained. A journalistic source is a person who provides the material intending the recipient to use it for the purpose of journalism or knowing it is likely to be so used. Where material is created or acquired with the intention of furthering a criminal purpose, the material is not to be regarded as having been created or acquired for the purposes of journalism. The likelihood of a local authority dealing with either of these issues is highly unlikely.

4.6 Items Subject to Legal Privilege

In general, communications between professional legal advisers and their clients are subject to legal privilege unless they are intended for the purpose of furthering criminal acts. The acquisition of material subject to legal privilege is particularly sensitive and may give rise to issues under Article 6 ECHR (right to a fair trial) as well as engaging Article 8 ECHR. As such, any covert surveillance of a lawyer known to be acting in their professional capacity should be assumed to fall in scenario (b) below. There are three scenarios where legally privileged items will or may be obtained:

(a) Where privileged material is intentionally sought;
(b) Where privileged material is likely to be obtained; and
(c) Where a purpose is to obtain items that, if they were not generated or held with the intention of furthering a criminal purpose, would be subject to privilege.

4.6.2 All three scenarios relate to the acquisition of privileged material during legal consultations which constitutes intrusive surveillance which as set out above, local authorities are prohibited from doing, hence no further details are required.

5. Additional Surveillance matters (outside of RIPA)

5.1 Activity Not Falling Within The Definition Of Covert Surveillance

5.1.1 The effect of RIPA Section 80 is to make authorised surveillance lawful, but it does not make unauthorised surveillance unlawful. The Council reserves the right to exercise it discretion regarding an investigation to determine that an alternative view or approach is required where the operation lies outside of the RIPA regime and controls. In such cases where the Crime Threshold is not met, the Council will adhere the Non-RIPA Surveillance Protocol and create and maintain written logs of activity which will be made available to internal and external oversight by IPCO.

5.1.2 Activity including immediate response to events; routine patrols (general observation activities), observation at trouble "hotspots;" covert surveillance not covered by a statutory ground in RIPA; overt use of CCTV and ANPR are all techniques not requiring RIPA authorisation.

5.1.3 Certain surveillance does not constitute either intrusive or directed surveillance. In the following scenarios, either an authorisation cannot be granted due to the specific circumstances, or an authorisation is not required BUT all such activity is permitted:

5.2 General Observation Activities

5.2.1 General observation duties whether overt or covert do not require RIPA authorisations as they form part of the legislative functions of public authorities as opposed to pre-planned surveillance of a specific person or group. At that stage there is not a specific investigation and instead the intention is through reactive enforcement to identify potential offenders. As part of this general duty of a public authority, the obtaining of private information is unlikely and so a DS authorisation is not required

5.3 Surveillance not relating to specific grounds or core functions

5.3.1 RIPA is required by public authorities who wish to carry out "core functions," which are specific public functions as opposed to "ordinary functions," undertaken by all authorities such as employment and contractual issues. Ordinary functions do not fall under the remit of RIPA as they are covered by the Data Protection Act 2018 and the Information Commissioner's Employment Practices Code.

5.3.2 If a Council employee is suspected of undertaking additional employment during work hours, or during sick or annual leave and the Council wishes to carry out covert surveillance outside of the employee's Council role, whilst there is a high likelihood of obtaining private information about the staff member, the surveillance would not constitute DS, as is it relates to the Council's ordinary functions, namely employment and contractual obligations, which are not core functions.

5.3.3 If a Council employee is on long term paid sick leave for injuries alleged to have been sustained during his employment and it is suspected the employee has had exaggerated and/or fabricated the purported injuries, the application for and receipt of full sick pay gives rise to the potential criminal offence of fraud. If the Council wished to carry out DS to ascertain if the employee is injured as declared or at all, the proposed investigation would relate to a core function of the Council , and the proposed DS is likely to result in obtaining private information. Accordingly, a DS authorisation should be considered and is required.

5.4 Overt Surveillance Cameras – CCTV & ANPR (Automatic Number Plate Recognition)

5.4.1 The Council's overt CCTV is governed by the Surveillance Camera Code of Practice and overseen by the Biometrics & Surveillance Camera Commissioner. The Code provides a framework of good practice including the processing of personal data and a public authority's duty to comply with Human Rights Act 1998. Please note the remit of surveillance cameras and the Council's cctv_code_of_practice_-_2020 regarding third party requests for use of the Council's CCTV.

5.5 Specific Situations – Authorisations Not Available

5.5.1 The following examples do not constitute directed or intrusive surveillance, but such activity is permitted:

5.5.1.1 Use of a recording device by a CHIS for which a conduct authorisation permitted the recording of any information already exists;

5.5.1.2 Overt or covert recording of the interview of a member of the public in a voluntary interview conducted by a public authority;

5.5.1.3 Covert recording of noise where the recording is decibels only nor non-verbal noise such as music, machinery or the recording of verbal content is made at a level that does not exceed that which can be heard on the street outside or adjoining property with the naked ear;

5.5.1.4 Entry on or interference with property or wireless telegraphy (not permitted by local authorities);

5.6 Combined Authorisation

5.6.1 Combined authorisations are permitted but are less likely to occur within the Council due to local authority restrictions and prohibitions regarding of certain surveillance categories.

5.7 CCTV Third Party Requirements

5.7.1 A third party (other agency e.g., the police) may request the Council to undertake surveillance for them by using the Council's resources, for example CCTV. Directed Surveillance requests to access/use the Council's CCTV must comply with the Council's CCTV Code of Practise. The Council will only permit the Police and other third parties to use its CCTV systems to carry out targeted covert surveillance (which includes the disclosure of recordings) if the requirements of the Code are adhered to.

5.7.2 An example would be where the police request the use of the Council's overt CCTV cameras by diverting and directing them for a pre-planned, specific investigation, focusing on access points and an adjacent alleyway, where intelligence indicates that a drug den is operating in a vacant commercial property nearby.

5.7.3 The police's intended directed surveillance is to be used in a manner that is likely to result in obtaining private information and the police must obtain a directed surveillance authorisation which specifically includes the required use of the Council's CCTV system. However, if an armed robbery took place and whilst the police were in pursuit of the suspect, they required urgent assistance to track the suspect's route to locate and arrest them, the police's request to divert and utilise the Council's overt town centre CCTV is an immediate response to an event hence, a DS authorisation application is not practicable and is therefore not required.

5.7.4 If any officer is in doubt as to how to proceed, please consult the Senior Responsible Officer at the earliest opportunity.

5.8 Consequences Of Non-Compliance With RIPA

5.8.1 Where covert surveillance is proposed for activity falling within the ambit of RIPA, this Policy and Processes must be strictly adhered to, to protect both the Council and individual officers from the following:

5.8.1.1 Evidence Rendered Inadmissible:
If covert surveillance is not lawfully undertaken the evidential product obtained may be deemed inadmissible by a trial judge in criminal proceedings, because the prejudicial effect of adducing it outweighs any probative value.

5.8.1.2 Legal Challenge:
Article 8 ECHR establishes a "right to respect for private and family life, home and correspondence". Any potential breach could give rise to an application for Judicial Review proceedings in the High Court by the aggrieved person or claim in the Investigatory Powers Tribunal.

6. RIPA Process

6.1 Mandatory URN

6.1.1 If DS satisfies the Crime Threshold Test or for a CHIS, officers must first obtain a Unique Reference Number [URN] for the operation from the SRO responsible for the Centrally Retrievable Record of Authorisations (**Appendix 4**) , prior to the completion and/or submission of an application for DS or CHIS to an (AO).

6.2 RIPA URN Request From

6.2.1 The applicant/officer must answer the following six questions within the RIPA URN Request Form (**Appendix 10**)

(a) Is DS/CHIS for the prevention or detection of Crime or disorder?
(b) If so, specify the criminal offence(s) being investigated and the statute(s);
(c) For Directed Surveillance only, does the criminal offence(s) being investigated meet the Crime Threshold Test (punishable with a period of at least six months imprisonment); or
(d) Does the offence(s) relate to the underage sale/supply of alcohol or tobacco/nicotine?
(e) Is the proposed covert surveillance both necessary and proportionate?
(f) Have you considered collateral intrusion and how this could be minimised?

6.2.2 The completed RIPA URN Request Form must be emailed to the Officer responsible for the Centrally Retrievable Record of Authorisations. Once the RIPA URN Request Form is received, considered, and satisfied, an URN will be allocated. All relevant information from this form must be inputted in the Centrally Retrievable Record of Authorisations and completed RIPA URN Request Form emailed to the applicant and named AO.

6.3 Required Forms

6.3.1 All RIPA forms are to be accessed from the Home Office website.

6.4 Application

6.4.1 The application form should be submitted to an AO from the list of certified Aos. The Applicant should ensure the Application sets out all relevant facts. It is not permitted to leave aspects of the application to be provided orally by the Applicant or to be solely contained in supporting documents.

6.4.2 All applications should be completed and authorised in a bespoke form rather than cutting and pasting the basis for the application or reasoning for the decision from previous applications. Best practice for all authorisations permitted by local authorities is contained in the Code;

- The reason why the authorisation is necessary and proportionate;
- Where a specific investigation or operation is involved, the nature of that investigation;
- For Directed Surveillance, the crime(s) being investigated that satisfy the Crime Threshold Test;
- CHIS applications should include the purpose for which the CHIS will be tasked or deployed;
- CHIS applications should include the nature of what the CHIS conduct will be;
- Details of potential collateral intrusion and why it is justified;
- Details of any material subject to legal privilege or other confidential information that may be obtained as a consequence of the authorisation;
- Applications should avoid repetition of any information;
- Information contained in applications should be limited to that required by the relevant legislation and code;
- The case for an authorisation should be presented in the application in a fair and balanced way and all reasonable efforts should be made to take account of information which supports or weakens the application for authorisation;
- An application should not require the sanction of any person other in a public authority other than an AO;
- Where it is foreseen, that other agencies will be involved in carrying out the surveillance, these agencies should be detailed in the application;
- Authorisations should not generally be sought for activities already authorised;

6.5 Authorisation

6.5.1 Officers must obtain both an internal authorisation of the application/renewal by an AO and Judicial Approval. To avoid any suggestion that any form has been simply signed off by an AO it is recommended that a copy is retained with the AO's wet signature i.e., original handwritten one, not merely a typed or electronic signature. The Council must be ready and able to provide the relevant witness if authenticity is ever questioned in Court.

6.6 Judicial Approval

6.6.1 An authorisation or renewal for Directed Surveillance or a CHIS is not activated until Judicial Approval is granted by a Magistrate and is both dated and timed.

6.7 Officers Authorised to apply for Judicial Approval

6.7.1 The Council has a list of authorised officers who are lawfully permitted to appear on behalf of the Council to apply for Judicial Approval **(Appendix 6).** It is anticipated that the officer will be the Applicant of the authorisation and Judicial Approval Application, as they will have full knowledge of the application and intended surveillance operation.

6.8 Judicial Approval Outcomes

6.8.1 There are 3 potential outcomes

(a) Application Granted [effective from that date and time];

(b) Refuse to grant or renew the Authorisation [Applicant can then re-apply once the gap/error has been corrected];

(c) Refuse to grant or renew the Authorisation and quash the AOs Authorisation.

6.8.2 Note: the Magistrate can only quash the Authorisation if the Applicant has had at least 2 business days' notice, from the date of refusal, in which to make representations against the refusal.

6.9 Duration

6.9.1 The period of validity for all authorisations commences on the date Judicial Approval is granted, not the date the Authorising Officer approved the application. The duration of the authorised surveillance is as follows:

6.9.1.1 Directed Surveillance : 3 months
6.9.1.2 CHIS: 12 months
6.9.1.3 Juvenile CHIS: 4 months (see review requirements)

6.10 Reviews

6.10.1 Regular reviews of all authorisations are required, the frequency of which should be determined and timetabled by the AO, once the authorisation has been granted and Judicial Approval obtained. The results of the review should be recorded in the Centrally Retrievable Record of Authorisations.

6.11 Directed Surveillance

6.11.1 Any proposed or unforeseen changes to the nature or extent of the activity which may result in further or greater intrusion into the private life of any person such as an additional person who has been identified as being an associate of the main subject, should also be brought to the attention of the AO by way of a review. The AO should consider if the proposed changes are proportionate before approving or rejecting them and any changes must be highlighted at the next renewal if one is required

6.11.2 If the identity of an individual becomes known during the course of directed surveillance, the terms of the authorisation should be amended at review to include the identity of the individuals and it would be appropriate to convene a review specifically for this purpose. Where the surveillance provides access to confidential information or involves collateral intrusion, the AO should conduct regular more frequent reviews.

6.12 CHIS

6.12.1 Where a CHIS authorisation provides for interference with the private or family life of initially unidentified individuals whose identity is later established, a new authorisation is not required provided the scope of the original authorisation envisaged interference with the private or family life of such individuals and this should be highlighted at renewal. Further, if the nature or extent of intrusion into the private or family life of any person becomes greater than anticipated at the original authorisation, the AO should immediately review the authorisation and reconsider the proportionality of the operation which should then be highlighted at renewal.

6.12.2 A juvenile CHIS authorisation is valid for 4 months but there is a requirement to review the authorisation at not less than monthly intervals to ensure it is maintained for no longer than necessary. The monthly reviews will take into account the operational case for maintaining the deployment and will also consider the impact on the mental and physical welfare of the young person.

6.13 Renewals

6.13.1 Renewals are permitted more than once, and the fact and outcome should be recorded in the Centrally Retrievable Record Authorisations. The AO must consider the application afresh including taking into account the benefits of the surveillance undertaken to date and any collateral intrusion that has occurred. If the application has resulted in the obtaining of confidential or legally privileged items, this fact should be highlighted in the renewal application.

6.13.2 Please note an authorisation will automatically expire unless a Renewal Application is made prior to its expiration and Judicial Approval is obtained. Applicants and AOs should be proactive about diarising, renewing, and cancelling authorisations as appropriate.

6.14 Cancellation

6.14.1 The officer has a duty to request the AO to cancel the authorisation when it no longer meets the criteria upon which it was originally authorised. If the original AO is no longer available, this duty falls to the person who has taken over the role or the person acting as the AO.

6.14.2 An example would be where a DS authorisation was obtained in order to conduct test purchases which were completed within 21 days. Consequently, the authorisation is no longer required, and it is bad practice to simply let the authorisation run to the automatic expiration date. Therefore, as soon as a decision is taken to discontinue the authorisation, the instruction must be given to those involved to stop all surveillance of the subject(s) as soon as reasonably practicable.

6.14.3 The RIPA cancellation form must be completed by the officer, authorised by the AO and the original form must be provided by hand (see above) to the SRO, following which the Centrally Retrievable Record Authorisations must be updated. It is good practice that a record should be retained detailing the product obtained from the surveillance and whether or not the objectives were achieved.

6.15 RIPA Documentation - Centrally Retrievable Records

6.15.1 The SRO is also required to ensure the following is obtained and retained for all covert surveillance operations the following, in a restricted location:

(a) RIPA URN Request Form;
(b) All original applications, any supplemental documentation, and the authorisations;
(c) Copy of the granted Judicial Approval Form; (Application/Renewal);
(d) Copy of the Order granting Judicial Approval (Application/Renewal);
(e) A record of the period over which the surveillance has taken place;
(f) The frequency of reviews prescribed by the AO;
(g) A record of the result of each review;
(h) A copy of any renewal of an authorisation together with the supporting documentation submitted when the renewal was requested;
(i) The date and time when any instruction to cease surveillance was given;
(j) The date and time when any other instruction was given by an AO.

6.15.2 AOs or officers must provide by hand all original RIPA forms to the SRO within 7 days of grant in a double sealed envelope marked "OFFICIAL - Strictly Private & Confidential" and/or email a scanned copy it to the SRO via the email address. The Judicial Approval Applicant must similarly provide the SRO by hand the original Judicial Approval granted/refused Form within 7 days of grant in a sealed envelope marked "Strictly Private & Confidential," and/or email a scanned copy to the SRO via the email address.

6.16 Retention of Records

6.16.1 Records must be available for inspection by the Investigatory Powers Commissioner and for the Investigatory Powers Tribunal (IPT). Please note the IPT will consider complaints made up to one year after the conduct to which the complaint relates to and may consider older or ongoing complaints where equitable to do so. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to six years.

7. RIPA Safeguards

7.1 Dissemination

7.1.1 Dissemination must be limited to the minimum necessary for authorised purposes if the material:

(a) is or is likely to become necessary for any of the statutory purposes set out in RIPA in relation to covert surveillance;

(b) is necessary to facilitate the carrying out of the functions of the public authorities under RIPA;
(c) is necessary for facilitating the carrying out of any functions for the Commissioner of IPT;
(d) is necessary for the purposes of legal proceedings; or
(e) necessary for the performance of the functions of any person by or under any enactment

7.1.2 In addition to limiting the number of persons to whom the material should be disseminated, there are also restrictions of the extent of the material disseminated for example, providing a summary of the material rather than copies of all authorisations and/or logs regarding the remit of the operation and evidence obtained. Please note, RIPA does not prevent material obtained under Directed Surveillance authorisations from being used to further any other investigations where it becomes relevant and in accordance with the safeguards required by the Code.

7.2 Use of Material as Evidence

7.2.1 Subject to the statutory framework governing the admissibility of evidence material obtained from directed surveillance or a CHIS is admissible as evidence in criminal proceedings. It is therefore vital for officers to ensure there is evidential integrity of the product obtained from the covert surveillance operation and the product is retained in accordance with the disclosure regime (see below).

7.3 Handling Material

7.3.1 All public authorities are required to have internal arrangements for the dissemination, copying, storage and destruction of private information obtained through covert surveillance. Further, the personal data obtained must be safeguarded by the AO and Data Controller in accordance with the Data Protection Act 2018 and the Council's Data Protection Policy including the necessity to report breaches to the Information Commissioner.

7.4 Copying Material

7.4.1 Copying material obtained from covert surveillance including summaries and extracts of the material is only permitted in accordance with the dissemination necessity principles (see above).

7.5 Storage of Material

7.5.1 All material obtained through covert surveillance and any copies/extracts from it must all be handled and stored securely to minimise the risk of loss or theft. Material must not be accessible to officers not connected to the operation or officers connected but to the operation but not authorised by the Officer in Charge to have access to it.

7.6 Destruction of Material

7.6.1 Information obtained through covert surveillance and all copies, extracts, 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). If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. Please note, if the material is necessary for the purposes of legal proceedings, in particular a prosecution, the disclosure regime must be complied with regarding the retention of material.

7.7 Protection of the identity of a CHIS

7.7.1 All organisations have a responsibility to protect the identity of those working as a CHIS and others who may be affected by the disclosure of the CHIS's identity. Attempts to protect the identity of the CHIS's must be made using all reasonable and lawful means possible and where appropriate, neither confirming or denying (NCND) the existence of or identity of the CHIS.

7.7.2 There are well-established legal procedures under Public Interest Immunity (PII) or closed material procedures that can be applied when seeking to protect the fact and identity of a CHIS from disclosure which would be dealt with by Legal Services and prosecution counsel in conjunction with the AO, as the Council would be the prosecuting authority.

PART B: IPA 2016, Acquisition of Communications Data

8. Acquisition of Communications Data

8.1 Statutory Authority

8.1.1 The Investigatory Powers Act 2016 (IPA), as amended by the Investigatory Powers (Amendment) Act 2024 and the Communications Data Code of Practice 2025 provide the statutory framework for the lawful acquisition of communications data (CD) by relevant public authorities. Local authorities are deemed to be a relevant public authority

8.2 Investigatory Powers Commissioner's Office (IPCO)

8.2.1 The Investigatory Powers Commissioner's Office is responsible for the independent authorisation and oversight of CD requests.

8.3 Communications Data Definition

8.3.1 Communications Data is information about communications: the "who," "when," "where," "when" "how," and "with whom," of a communication but not what was written or said (the content). Generally, CD is acquired from a Telecommunications Operator (TO), the definition of which is extensive.

8.4 Categories of Communications Data

8.4.1 All communications data held by a telecommunications operator or that which is obtainable from a telecommunications system now falls into two categories of CD.

8.4.2 Entity Data

8.4.2.1 Entity data is about entities or links between them and describes or identifies the entity but does not include information about individual network events which those entities are involved in. Entities could be individuals, groups and objects (such as mobile phones or other communication devices). Entity data can change over time if for example someone moves house, the address held by a TO will be updated and changed. This category of CD broadly replaces subscriber data and includes:

(a) Subscriber information: identify of the person to whom the services are provided
(b) Subscriber checks: who is the subscriber of the phone number 01234 567890
(c) Subscriber/account holder: names, address of installing, billing payments etc.
(d) Connection/disconnection: what the account holder is allocated or has subscribed to Reconnection information
(e) Apparatus/device information: e.g. VIN Vehicle Identification Number when linked with a SIM card imbedded within a vehicle
(f) PUK Code: Personal Unlocking Key code for SIM cards

8.4.2.2 Events data identifies or describes time bound events taking place across a telecommunications system (TS), limited to communication events describing the transmission of information between two or more entitles over a TS. Events data includes the following details regarding the communication:

(a) Date and time sent
(b) Duration
(c) Frequency;
(d) Call diversion;
(e) IP address;
(f) Information tracing the origin or destination of a communication that is or has been in transmission;
(g) Sender or recipient of a communication
(h) Information identifying the location of apparatus when a communication is, has or may be made or received (e.g., the location of a mobile phone);
(i) Itemised telephone call records;
(j) Volume of data downloaded and/or uploaded;
(k) Use of services i.e., conference calling, call messaging, call waiting

8.5 Local Authority Prohibitions

8.5.1 The Local Authority is prohibited from;

8.5.1.1 obtaining the content of any communication i.e., what was said or written;

8.5.1.2 acquiring the Internet Connection Records (ICRs)

8.6 Two Mandatory Tests for Communications Data Requests

8.6.1 Necessary

8.6.1.1 Local authorities are only permitted to internally grant and seek external authorisation from NAFN and thereafter IPCO if and only if they are necessary for the applicable crime purpose.

8.6.1.2 Applicable Crime Purpose test depends on whether the CD being sought is entity or events data:

(a) where the communications data is wholly or partly events data, the purpose of preventing or detecting serious crime;

(b) in any other case, the purpose of preventing or detecting crime or preventing disorder; Serious Crime Threshold – Applicable to Events Data Only

8.6.1.3 Serious Crime Threshold – Applicable to Events Data Only, offences that satisfy the threshold are:

(a) An offence capable of attracting a prison sentence of 12 months or more (for persons 18+ in England)

(b) An offence by a person who is not an individual (i.e., corporate body);

(c) An offence which involves, as an integral part of it, the sending of a communication;

(d) An offence which involves, as an integral part of it, a breach of a person's privacy;

(e) An offence falling within the definition of serious crime (i.e., where the conduct involves the use of violence, results in substantial financial gain or is by a large number of persons in pursuit of a common purpose);

8.6.2 Proportionate

8.6.2.1 The conduct the subject matter of the Application must be proportionate to what is sought to be achieved.

9. Key Roles (IPA – Communications Data)

9.1 Senior Responsible Officer (SRO)

9.1.1 The Council's Senior Responsible Officer (SRO) is the Council's Executive Head of Governance & Law. The Communications Data Code of Practice specifies the SRO is responsible for:

(a) the integrity of the process in place within the public authority to acquire communications data;

(b) engagement with authorising officers in IPCO; IPA; Code of Practice, including responsibility for novel or contentious cases;

(c) oversight of the reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;

(d) ensuring the overall quality of applications submitted to IPCO;

(e) engagement with the IPCO's inspectors when they conduct their inspections; and
(f) where necessary, oversight of the implementation of post-inspection action plans approved by the IPC

9.2 Designated Senior Officer (DSO)

9.2.1 A Designated Senior Office (DSO) for local authorities must be an individual who holds the position of director, head of service or service manager (or equivalent); or a high position, which mirrors the rank required for RIPA AOs. The Council's DSOs are listed in **Appendix 3**.

9.2.2 A DSO must be independent from the operations or investigations and so should be far enough removed from the applicant's line management chain or the investigation so as to not be influenced by operational imperatives, such as pressure to expedite results on a particular operation. The DSO should therefore not be within the same department or unit or an integral part of the investigation. It is not considered good practice for applicants to be able to choose a designated senior officer on a case-by-case basis. Accordingly, the DSO should be selected from a different department.

9.3 NAFN – Local Authorities

9.3.1 All local authorities wishing to acquire CD must be members of and use NAFN throughout the application process via their online portal. The council must ensure the DSO is aware the application is being made before it is submitted. The Council's CD Single Point of Contact (SPOC) listed in **Appendix 9** will assist the DSO and Applicant where required. NAFN's role includes provision of advice to the Applicant officer including:

(a) Whether it is reasonably practical to obtain the data;
(b) Interpretation of IPA, particularly whether an authorisation is appropriate;
(c) Ensure authorisations are lawful under IPA and meet the Serious Crime Threshold Test for Events Data requests;
(d) Possible unintended consequences of the application such as excess data; sensitive professions and collateral intrusion;
(e) Why the service(s) recommended support the objective(s) of the investigation;
(f) Add value in comments, considerations and recommendations as prescribed in the Code of Practice under the roles and responsibilities of the SPOC;
(g) Where appropriate, flag any issues regarding quality assurance of the application to be remedied before submission of the application;
(h) Monitor applications returned for rework or rejected by IPCO and determine the reasons why;
(i) Provide organisational and/or individual training as and where necessary, sharing best practice advice and support;

9.3.2 NAFN must be provided coverage for all CD acquisitions they intend to make and if the Application passes NAFN's assessment, NAFN will then submit it to IPCO for consideration of authorisation.

10. Key Terms

10.1 Telecommunications Operator (TO)

10.1.1 A person who offers or provides a telecommunications service to persons in the UK or controls or provides a telecommunications system which is wholly or partly in the UK or controlled from the UK. TO's may provide applications, websites (chat function not required) or some interface with the internet that facilitates electronic signals being sent between persons or things.

10.2 Content

10.2.1 Content is any element of a communication, or the data attached to it or associated with it that might reasonably be considered to be the meaning of the communication. Obtaining such information would constitute Targeted Intercept which local authorities are prohibited from obtaining.

10.3 Postal Operator (PO)

10.3.1 Postal items include letters, postcards, packets, and parcels and therefore the remit of postal operators includes companies beyond the Post Office such as Amazon, DPD etc.

10.4 Postal Definitions

10.4.1 Communications data in relation to a postal service has 3 elements:

(a) Postal data which is or has been compromised in or attached to the communication for the purpose of the service which it was transmitted;
(b) Data relating to the use made by a person of a postal service;
(c) Information held or obtained by a postal operator about persons to whom the postal operator provides or has provided a communications service, and which relates to the provision of the service

10.5 Internet Connection Records (ICRs)

10.5.1 An ICR provides details of the internet service that a specific device has connected to (e.g., a website or instant messaging application). Please note local authorities are prohibited from obtaining ICRs.

10.6 Third Party Data

10.6.1 Where a communication is sent there may be multiple providers involved in the delivery of the communication and each provider may require different elements of communications data to route the communication. For example, when sending an email there will be the email provider, the internet access provider for the sender and the internet access provider for the recipient.

10.6.2 Where one TO is able to see or access the communications data in relation to applications or services running over their network, in the clear, but does not process that communications data in any way this is regarded as third party data. A TO is considered to process data if it specifically looks at an item of data in order to determine what action to take or it has a specified process.

10.6.3 A communications data authorisation may be given for the acquisition by a public authority of third party data on a forward looking basis where necessary and proportionate in relation to a specific investigation. A TO or PO need only obtain and disclose third party data where reasonably practicable to do so. Where such data is encrypted by the third party a telecommunications operator is under no obligation to decrypt such information.

10.7 Collateral Intrusion

10.7.1 The risk of obtaining communications, equipment data or other information about nontargets. Each Application should identify the risk of collateral intrusion and specify what steps will be undertaken to reduce it.

10.8 Journalistic Sources

10.8.1 The only category of CD which requires local authorities to first obtain authorisation and approval by an IPCO Judicial Commissioner is where the purpose of a CD application is to identify a journalistic source. The Applicant and SPOC should pay special consideration to these applications and inform their DSO.

10.9 Novel Or Contentious Circumstances

10.9.1 Due to ongoing improvements in technology, there will be circumstances where the potential acquisition of CD may be considered novel or contentious. In such circumstances, public authorities are permitted to see guidance from IPCO prior to progressing any conduct to acquire CD.

11. Acquisition Of Communications Data Process

11.1 National Prioritisation Grade (NPG)

11.1.1 The CD Application must include the NPG which will be independently assessed by NAFN, to assist IPOC as to the operational urgency. There are four prioritisation categories and local authorities are only permitted to use Priorities 2-4:

11.1.2 See Table.

IPCO PRIORITIES - OPERATIONAL PRIORITISATION	**DEFINITION**
Priority 1	
Immediate Threat to Life or Serious Harm	**Not applicable to local authorities**
Priority 2	
Urgent Operational Necessity (6 working hours)	The urgent acquisition of CD will directly assist the **prevention or detection of the commission of a serious crime, or the making of arrests or the seizure of illicit material, or where there the operational opportunity will be lost.** Or any of the scenarios described for Priority 1 which whilst urgent do not require immediate action
OPERATIONAL PRIORITISATION	**DEFINITION**

Priority 3	
Routine **(Time Critical Enquiry)** (1 working day/15 working hours)	Not urgent but include specific or time critical issues such as bail or court dates or where a specific line of investigation into a serious crime and early acquisition of CD will directly assist in the prevention or detection for that crime or safeguarding and preservation of human life
Priority 4	
Routine (6 working days)	Matters that support a specific line of investigation into a crime or incident but are not urgent and do not meet any time critical issues. The acquisition of CD as a matter of course will assist in that investigation

11.2 Category Of Communications Data Required

11.2.1 Consideration must be given at the outset as to whether Entity or Events Data is required. Usually, it is appropriate to start with obtaining entity data to confirm information within the investigation. However, if there is sufficient information known at the outset, it may be appropriate to request Events Data first. For example:

(a) a victim reports receiving nuisance or threatening telephone calls or messages;
(b) a person who is the subject of an investigation or operation is identified from intelligence to be using a specific communications service;
(c) a victim, a witness or a person who is the subject of an investigation or operation has used a public payphone;
(d) a mobile telephone is lawfully seized, and communications data is to be acquired relating to either or both the device or its SIM card(s);

11.3 Application

11.3.1 Officers should complete a Communications Data Application form on NAFN's portal, ensuring it is clear as to whether the application is for Entity or Events Data; is necessary; that it satisfies the Applicable Crime Purpose test; and for Events Data that it also satisfies the Serious Crime Threshold Test. All Applications must also be proportionate and the Application to acquire CD must:

(a) describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
(b) specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
(c) include a unique reference number;
(d) include the name and the office, rank or position held by the person making the application;
(e) describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person, or other person relevant to the investigation or operation;
(f) include the operation name (if applicable) to which the application relates;
(g) identify and explain the time scale within which the data is required;
(h) address necessity and proportionality;
(i) present the case for the authorisation in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation;

(j) consider and, where appropriate, describe any meaningful collateral intrusion and why that intrusion is justified in the circumstances;
(k) consider and, where appropriate, describe any possible unintended consequences of the application; and
(l) where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

11.3.2 General guidance for Applications is:

(a) All addresses should be accurately validated based on source material before the completion of the application form by both the Applicant and SPOC
(b) Keep all applications simple, legal, and concise;
(c) Avoid acronyms and abbreviations unless explained first;
(d) Use standard terminology to describe the main subject in your application (e.g., victim, witness, complainant, suspect etc.);
(e) Clearly state the crime, offence, and purpose at the start of the Application;
(f) Be specific about daters of intelligence within the Application;
(g) Do not refer to another application, document, or system instead of addressing necessity and proportionality;
(h) Be specific about how you have or have tried to attribute the identifier (e.g., name/date of birth/home address/email address) to the person the subject of the Application;
(i) Clearly state the objective of your application. Do not name the services or products from the service provider;
(j) Always consider the victim's right of privacy when describing events within applications. These can be high level descriptions and do not need to contain graphic details of offences.

11.4 DSO Process

11.4.1 Before an application is submitted to NAFN, it must be brought to the attention of the DSO who has been given the designated role of overseeing the Applications before submission to NAFN. Guidance for DSO's when considering a CD Application is:

(a) Objectively review the application and the relevant individuals' right to privacy;
(b) Provide a bespoke authorisation avoiding use of standard phrases such as "the data should be held in accordance with the policy;
(c) Explicitly state the crime/offence understood to be the subject of the investigation;
(d) Clearly record having fully considered and understood the Application;
(e)
(f) Clearly record necessity and proportionality are understood and have been considered;

(g) Clearly record consideration has been given to any potential for the authorisation to result in unintended consequences (e.g., collateral intrusion);
(h) Specifically state how the service requested will support the objective outlined in the Application;
(i) For applications into certain professions, explicit consideration must be given and recorded regarding any unintended consequences of such applications and address whether the public interest is best served by the Application;
(j) If it is a novel or contentious Application, clearly explain why you consider the application to be so and include why this is considered to be a lawful request

11.4.2 Where an authorising individual does not consider the acquisition of communications data specified in the application to be necessary and proportionate, they may either seek further information from the applicant or refuse the request.

11.5 Submission to NAFN

11.5.1 Once the Application has been submitted on NAFN's portal, the DSSO will be notified and asked within the portal to confirm they are aware of the application.

11.6 IPCO's Refusal To Grant Authorisation

11.6.1 Where a request is refused by a IPC there are three options:
(a) not proceed with the request;
(b) resubmit the application with a revised justification and/or a revised course of conduct to acquire communications data;
(c) resubmit the application with the same justification and same course of conduct seeking a review of the decision by IPCO. A public authority may only resubmit an application on the same grounds to IPCO where the senior responsible officer or a person of equivalent grade in the public authority has agreed to this course of action. IPCO will provide guidance on its process for reviewing such decisions.

11.6.2 If NAFN refuse to submit the application to IPCO or IPCO refuse the Application for CD, the activity cannot commence.

11.7 Authorisation

11.7.1 An authorisation provides the following types of conduct may be authorised:

11.7.1.1 conduct to acquire communications data - which may include the public authority obtaining communications data themselves or asking any person believed to be in possession of or capable of obtaining the communications data to obtain and disclose it; and/or

11.7.1.2 the giving of a notice - allowing the public authority to require by a notice a telecommunications operator to obtain and disclose the required data.

11.7.2 An authorisation of conduct to acquire communications data may be appropriate where, for example

(a) there is an agreement in place between a public authority and a TO or PO to facilitate the secure and swift disclosure of communications data.
(b) where the data can be acquired directly from a telecommunication system and the activity does not constitute interception or equipment interference; or
(c) where a public authority considers there is a requirement to identify a person to whom a service is provided but the specific TO or PO has yet to be conclusively determined as the holder of the communications data.

11.8 Notices In Pursuance Of An Authorisation

11.8.1 The giving of a notice is appropriate where a TO or PO is able to retrieve or obtain specific data, and to disclose that data, and the relevant authorisation has been granted. A notice may require a TO or PO to obtain any communications data if that data is not already in its possession. The decision to authorise the issuing of a notice must be based on information presented in an application. Once IPCO has authorised the giving of a notice, it will be given to the TO or PO in writing. The notice should contain enough information to allow the telecommunications operator or postal operator to comply with the requirements of the notice. A TO or PO is not required to do anything under a notice which it is not reasonably practicable for it to do. A notice may only require a TO or PO to disclose the communications data to the public authority.

11.9 Duration

11.9.1 Once granted the CD authorisation is valid for one month.

11.10 Renewal

11.10.1 A renewed authorisation takes effect upon the expiry of the authorisation it is renewing. The renewal application will similarly have to be submitted to NAFN for its authorisation and onward submission to IPCO. Accordingly, the time required to complete this process must be factored in and back calculated from the current date of expiration.

11.11 Cancellations

11.11.1 The DSO granting the authorisation must cancel it if at any time after the grant of authorisation by IPCO, it is no longer necessary for a statutory purpose, or the conduct required by the authorisation is no longer proportionate to what was sought to be achieved.

11.12 Communications Data Centrally Retrievable Record

11.12.1 The Council CD electronic centrally retrievable register (CD CRR) is maintained by a Legal Services' Officer.

11.13 Record Keeping

11.13.1 A copy of the online Application/Review/Renewal or Cancellation form submitted online to NAFN must be retained and be provided to the SRO by hand, within 7 days, in a double sealed envelope marked "OFFICIAL SENSITIVE - Strictly Private & Confidential" and/or emailed to the SRO via the designated email. Due to the degree of sensitivity and risk arising from obtaining and retaining documents in a central database, IPCO only retains the CD applications for a limited period. Public authorities are therefore required to keep records of both CD applications issued and decisions received from IPCO. The Council has mirrored the retention period for covert surveillance documentation and will retain records for a period of six years.

11.13.2 Each relevant public authority must also keep a record of the following information:

(a) the number of applications submitted by an applicant to a SPOC seeking the acquisition of communications data;
(b) the number of applications submitted by an applicant to a SPOC seeking the acquisition of communications data, which were referred back to the applicant for amendment or declined by the SPOC, including the reason for doing so;
(c) the number of applications submitted to an authorising individual for a decision to obtain communications data, which were approved after due consideration by the DSO and thereafter by IPCO;
(d) the number of applications submitted to an authorising individual for a decision to obtain communications data, which were referred back to the applicant or rejected after due consideration, including the reason for doing so;
(e) the number of authorisations of conduct to acquire communications data granted by the DSO and thereafter IPCO;
(f) the number of authorisations to give a notice to acquire communications data granted by the DSO and thereafter ICPO
(g) the number of notices given pursuant to an authorisation requiring disclosure of communications data;
(h) the priority grading of the authorisation for communications data (see Operational Prioritisation Table above);
(i) whether any part of the authorisation relates to a person who is a member of a profession that handles privileged or otherwise confidential information (such as a medical doctor, lawyer, journalist, member of a relevant legislature, or minister of religion) (and if so, which profession);
(j) the number of times an authorisation is granted to obtain communications data in order to confirm or identify a journalist's source; and
(k) the number of items of communications data sought, for authorisation granted by a DSO and thereafter IPCO.

11.13.3 These records should distinguish between requests considered by IPCO and those considered by designated senior officers.

11.13.4 For each item of communications data (including consequential data) included within a notice or authorisation, the relevant public authority must also keep a record of data required by the Code, which is contained in the Council's Electronic Communications Data Centrally Retrievable Register (CD CRR) **Appendix 8**. If the advice of a Judicial Commissioner or IPC has been sought prior to the acquisition of communications data that could be considered novel or contentious, the fact and views of IPCP or the Judicial Commissioner will be recorded in the CD CRR. It is the responsibility of the Senior Responsible Office to maintain this record. These records must be sent in written or electronic form to the IPC, as requested by them.

12. IPA Safeguards

12.1 General Handling

12.1.1 In addition to the requirements of the data protection legislation, CD held by a public authority should be treated as information with a classification marking of Official with a caveat of Sensitive, though it may be classified as higher if appropriate. Communications data acquired under the Act and all copies, extracts and summaries of it, must be held in a manner which provides an adequate level of protection for the relative sensitivity of the data and meets the data protection principles outlined in relevant data protection legislation. All required documentation is to be provided to the SRO by hand within 7 days of grant in a double sealed envelope marked "OFFICIAL SENSITIVE - Strictly Private & Confidential" and/or emailed to the SRO via the designated email address. The SRO will retain all material in a secure location with access restricted to the SRO and officer responsible for maintaining the CD Centrally Retrievable Record. Details of the officer responsible for maintaining the centrally retrievable Communications Data (CD) register are provided in **Appendix 7**. The CD CRR should be retained for perpetuity.

12.2 Retention

12.2.1 Communications data may only be held for as long as the relevant public authority is satisfied that it is still necessary for a statutory purpose. When it is no longer necessary or proportionate to hold such data, all copies of relevant data held by the public authority must be destroyed. Data must be deleted such that it is impossible to access at the end of the period for which it is required. If such material is retained, it should be reviewed when appropriate to confirm that the justification for its retention is still valid for one or more of the authorised purposes. Records must be available for inspection by the Investigatory Powers Commissioner and for the IPT. Although records are only required to be retained for at least three years, it is therefore desirable, if possible, to retain records for up to six years.

12.3 Notification

12.3.1 Where communications data is being sought from a TO or PO, if either the TO or PO is permitted to notify the subject(s) of the fact that a request has been made for their data the relevant public authority must specify this when requesting the data. The public authority must, at the point of application, consider whether it would be damaging to investigations to notify the individual that their data will be acquired. Please note, if the CD is required for the purpose of a criminal investigation, care must be taken not to tip the subject off prior to the completion of the investigation and outside of the formal pre- interview disclosure and/or disclosure process (see below).

12.4 Notification of Serious Errors

12.4.1 If the CD is wrongly acquired or disclosed, the public authority making or establishing an error has been made must report the error to the SRO and IPC. The criteria for the IPC to notify an individual of the error is that it is a serious error and it is in the public interest for the individual concerned to be informed of the error. If the person is informed, they must be informed of their right to apply to IPT.

12.5 Notification of acquisition in criminal proceedings

12.5.1 Where communications data has been acquired during the course of a criminal investigation that comes to trial an individual will be made aware, in most cases, that data has been obtained. Where communications data is used to support the prosecution case it will be served as evidence on the defendant. Additionally in compliance with its disclosure the prosecution will reveal the existence of communications data (and potentially the material generated in the process of it being obtained) to a defendant on a schedule of non-sensitive unused material if that data is relevant. Please see Disclosure Duties & Obligations for further guidance.

12.6 Compliance & Offences

12.6.1 It is an offence for a person without lawful authority to knowingly or recklessly obtain CD from a TO or PO. It is a defence to show the person acted in the reasonable belief that the person had lawful authority to obtain the CD.

Part 3: Shared Duties, Obligations and Oversight (RIPA & IPA)

13. RIPA &IPA Oversight

13.1 Approval of Policy

13.1.1 The Council's RIPA & IPA Policy and Processes is submitted to Cabinet for its approval.

13.2 Annual Review of Policy

13.2.1 The Code requires a review of the Policy at least annually. The SRO is responsible for preparing the annual RIPA & IPA Report and Review of the RIPA & IPA Policy to the Audit & Resources Committee which provides members the basis to consider and review the adequacy of the Council's RIPA & IPA Policy. The Code also recommends elected members consider internal reports on the use of RIPA and CD on a regular basis, to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. Accordingly, following each annual RIPA/IPA Bi-Annual meeting the SRO will prepare an internal report to the elected members as to the content and outcome of the meeting.

13.3 Designated Officers Annual Meetings

13.3.1 This meeting is to be chaired by the SRO for designated officers to ensure relevant updates to the statutory framework and any issues arising from the SRO's internal monitoring of the RIPA CRR are addressed and remedied in a timely manner. As set out above the SRO will prepare and submit an internal Report to the elected members following the annual meeting

13.4 Internal Monitoring

13.4.1 The SRO will undertake an internal reviews and audit of the RIPA Centrally Retrievable Record (CRR) and the CD Centrally Retrievable Record not less than quarterly. The SRO will also identify any issues arising from the internal audit and raise such issues at the RIPA bi-annual meeting with AOs to address and resolve the live issues. Any urgent matters should be raised with the AO's as soon as is possible and, in any event, prior to the next meeting.

13.5 Training

13.5.1 All new AOs and DSOs are appointed by the SRO who will ensure all AOs and DSOs attend suitable training and refresher courses. All Council officers utilising RIPA and/or IPA must also have attended a suitable training and refresher courses. Whilst undertaking the internal audits of the RIPA CRR, the SRO will also identify any training needs for staff and/or monitoring issues to be raised with individual AO's and/or at a RIPA & IPA bi-annual Meeting. Additionally, the SRO will provide RIPA and IPA updates/advice notes and briefings to all relevant staff when required.

13.6 Codes of Practice

13.6.1 The Home Office publishes Codes of Practice for Covert Surveillance & Property Interference; CHIS; Communications Data and the Surveillance Camera. Public authorities like the Council may be required to justify the use, granting or refusal of authorisations by reference to the Codes. If any officer is uncertain as to the meaning or application of any aspect of the Codes, legal advice should be obtained from the SRO.

13.7 Investigatory Powers Tribunal (IPT)

13.7.1 The IPT is an independent body with full powers to investigate and decide any case within its jurisdiction. The IPT can order compensation, quashing of a warrant or authorisation or the destruction of any records of information held unlawfully.

14. Reporting to the Commissioner

14.1 Reporting Errors

14.1.1 Public authorities are expected to have thorough procedures in place to comply with RIPA. The SRO will undertake regular reviews of errors and a written record must be made of each review.

14.1.2 An error must be reported if it is a "relevant error," by a public authority in complying with any requirements that re imposed on it by any enactment which are subject to review by a Judicial Commissioner. Errors must be notified to the Investigatory Powers Commissioner as soon as is reasonably practicable and no later than ten working days after the error has been identified. Where the full facts cannot be ascertained within that time, an initial notification must be sent with an estimated timescale for the error being reported in full and an explanation of the steps being undertaken to establish the full facts of the error.

14.2 Serious Errors

14.2.1 IPCO is under a statutory duty to inform the 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 notified of the error. The error is deemed serious if the error has caused significant prejudice or harm to the person concerned. Factors to be considered when determining if it is in the public interest to inform the person of the error are;

(a) The seriousness of the error and its effect on the person concerned;
(b) The extent to which disclosing the error would be contrary to the public interest or prejudicial to:
(c) National security;
(d) The prevention or detection of serious crime;
(e) The economic well-being of the UK; or
(f) The continued discharge of the functions of any of the intelligence services;

14.2.2 The Commissioner must seek submissions from the public authority before deciding whether to inform the person regarding the error.

14.3 Investigatory Powers Commissioner’s Office (IPCO)

14.3.1 The Investigatory Powers Commissioner’s Office (IPCO) is the supervisory body for RIPA & IPA and following the merger with OCDA it deals with Communications Data authorisations as well as oversight.

RIPA & IPA POLICY - APPENDICES

APPENDIX 1: SENIOR RESONSIBLE OFFICER (RIPA & COMMUNICATIONS DATA)

NAME	POSITION	EMAIL
Amanda Bancroft	Executive Head of Governance & Law (Monitoring Officer)	Amanda.Bancroft@rushmoor.gov.uk

APPENDIX 2: RIPA AUTHORISING OFFICERS

NAME	POSITION
Ian Harrison	Chief Executive and Head of Paid Service
James Duggin	Chief Operating Officer
Nikki Fleming	Financial Governance Manager
Colin Alborough	Service Manager – Place

DRAFT

APPENDIX 3: COMMUNICATIONS DATA DESIGNATED SENIOR OFFICERS

NAME	POSITION
Ian Harrison	Chief Executive and Head of Paid Service
James Duggin	Chief Operating Officer
Nikki Fleming	Financial Governance Manager
Colin Alborough	Service Manager – Place

APPENDIX 4: OFFICER RESPONSIBLE FOR MAINTAINING RIPA CENTRALLY RETRIEVABLE REGISTER

NAME	**POSITION**
Amanda Bancroft	**Executive Head of Governance and Law**

APPENDIX 5: THE RIPA CENTRALLY RETRIEVABLE RECORD (template)

Unique reference number (URN) of the investigation	Name of Officer Completing Record of Authorisation	Type of authorisation or notice	Date provisional authorisation or notice was given	Name and rank/grade of the authorising officer	Is authorising officer directly involved in the investigation?	Date judicial approval was received or refused (add link to supporting application & authorisation decision)	Title of investigation or operation, including a brief description and names of subjects, if known	Whether the investigation or operation is likely to result in obtaining confidential or privileged information per code of practice	What surveillance product will result e.g. still imagery, video imagery (with or without sound), officer observations which will then be written into a report	If the authorisation or notice is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer and the date of judicial approval	Review Date (s)	Date the authorisation or notice was cancelled	Officer cancelling the authorisation or notice	Review of the surveillance product status (note the surveillance product should be destroyed as soon as no longer needed for investigatory purposes)	Other comments

APPENDIX 6: OFFICERS AUTHORISED TO APPLY FOR JUDICIAL APPROVAL

The following officers are authorised by the Council to apply for Judicial Approval for Directed Surveillance or CHIS:

NAME	POSITION
Amanda Bancroft	Executive Head of Governance and Law

APPENDIX 7: OFFICER RESPONSIBLE FOR MAINTAINING COMMUNICATIONS DATA (CD) CENTRALLY RETRIEVABLE REGISTER

NAME	POSITION
Amanda Bancroft	**Executive Head of Governance and Law**

APPENDIX 8: COMMUNICATIONS DATA CENTRALLY RETRIEVABLE REGISTER (template)

Unique CD Reference Number	Related Case / Investigation Ref	Date Entry Created	Applicant Name	Applicant Role / Service	Type o CD	Purpose o Request	Statutory Power (IPA 2016 Part 3)	Designated Senior Officer	Date of Authorisations	Judicial Approval Required (Yes/No)	Judicial Authority	Date Judicial Approval Granted/ Refused	SPoC	Communications Service Provider	Date Request Served	Date Data Received	Retention Period	Date Data Deleted

APPENDIX 9: COMMUNICATIONS DATA SPOC

NAME	POSITION
Amanda Bancroft	Executive Head of Governance and Law

APPENDIX 10: RIPA URN REQUEST FORM

RIPA URN REQUEST FORM

APPLICANT'S DETAILS	
Department Seeking URN	
Name of Officer Seeking URN	
Role of Officer Seeking URN	
TYPE OF COVERT SURVEILLANCE	
Directed Surveillance or CHIS	
SUBJECT	
Name of Subject or Location if specific subject not identified	
Is Confidential Information likely to be obtained?	
PRE-CONDITION TESTS	
Is DS/CHIS for the Prevention or Detection of Crime?	
Specify Criminal Offence(s) being investigated & statute(s)	
For Directed Surveillance Only: Does the Criminal Offence(s) satisfy the Crime Threshold Test? Or	
Is the offence(s) for the underage sale of alcohol/tobacco/ or underage sale and/or proxy purchasing of nicotine inhaling products	
APPLICATION	
Operation Reference	
Name of Authorising Officer	
Is the Authorising Officer directly involved in the Operation or Investigation?	
Is Confidential Information likely to be obtained?	
Was the Application granted?	
Was Judicial Approval Obtained?	
Date & Time of Judicial Approval Order	
Expiry Date	
URN	
URN issued	
Officer issuing URN	
Date & Time URN issued	
KEY DATES	
Authorised	
Judicial Approval	
Review	
Renewal	
Cancellation	