# EASTLEIGH BOROUGH COUNCIL

# CORPORATE POLICY AND PROCEDURES

# REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

# &

# INVESTIGATORY POWERS ACT 2016 (IPA)

**RESTRICTED**

## VERSION CONTROL

| Version | Date |
|---|---|
| 1 | January 2008 |
| 2 | July 2012 |
| 3 | July 2015 |
| 4 | February 2016 |
| 5 | January 2019 |
| 6 | February 2022 |
| 7 | April 2024 |

**INDEX**

## APPENDICES

| APPENDIX | TITLE |
|---|---|
| 1 | SENIOR RESPONSIBLE OFFICER |
| 2 | RIPA AUTHORISING OFFICERS |
| 3 | COMMUNICATIONS DATA SENIOR DESINGATED OFFICERS |
| 4 | OFFICER RESPONSIBLE FOR MAINTAINING RIPA CENTRALLY RETRIEVABLE REGISTER |
| 5 | RIPA CENTRALLY RETRIEVABLE REGISTER |
| 6 | JUDICIAL APPROVAL SPOC |
| 7 | JUDICIAL APPROVAL DESIGNATED OFFICERS |
| 8 | OFFICER RESPONSIBLE FOR MAINTAINING COMMUNICATIONS DATA CENTRALLY RETRIEVABLE REGISTER |
| 9 | COMMUNICATIONS DATA CENTRALLY RETRIEVABLE REGISTER |
| 10 | COMMUNICATIONS DATA SPOC |
| 11 | PROSECUTIONS SPECIALISTS |
| 12 | NAFN |
| 13 | ACRONYMS |
| 14 | RIPA CODES OF PRACTICE |
| 15 | RIPA URN Request Form |
| 16 | RIPA FORMS |
| 17 | JUDICIAL APPROVAL APPLICATION FORM B |
| 18 | JUDICIAL APPROVAL PROTOCOL BETWEEN EASTLEIGH BOROUGH COUNCIL & SOUTHAMPTON MAGISTRATES' COURT |
| 19 | JUDICIAL APPROVAL APPLICATION & HEARING GUIDANCE |
| 20 | COMMUNICATIONS DATA CODE OF PRACTICE |
| 21 | RIPA TRAINING REGISTER |
| 22 | IPA TRAINING REGISTER |
| 23 | RIPA FLOWCHART: DECISION PROCESS |
| 24 | COMMUNICATIONS DATA APPLICATION PROCESS |
| 25 | RIPA CCTV PROTOCOL |
| 26 | NON-RIPA SURVEILLANCE PROTOCOL |
| 27 | OFFICER RESPONSIBLE FOR NON-RIPA CENTRALLY RETRIEVABLE REGISTER |
| 28 | NON-RIPA CENTRALLY RETRIEVABLE REGISTER |
| 29 | NON-RIPA FORMS |
| 30 | COMMUNICATIONS DATA URN REQUEST FORM |
| 31 | NAFN COMMUNICATIONS DATA GUIDANCE APPLICATION FORM |
| 32 | PRO FORMA COMMUNICATIONS DATA APPLICATION FORM |

## (1) INTRODUCTION & KEY MESSAGES

1. This policy sets out the statutory framework and procedures which permit the Council's lawful use of covert surveillance techniques and the acquisition of Communications Data (CD) for use in an investigation.

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). Some rights are absolute whilst others are qualified, thus it is permissible for the state to interfere with those rights, provided certain conditions are satisfied. One of those rights is a person's right to respect for their private and family life, home, and correspondence.[1]

3. When public authorities seek to obtain private information about a person by means of covert surveillance Article 8 is the most likely to be engaged.

4. Regulatory Investigations Powers Act 2000 (RIPA) Part II provides the statutory framework to enable covert surveillance to be lawfully authorised and conducted and IPA [Investigatory Powers Act 2016] provides the statutory framework for the acquisition of Communications Data (CD) obtained by a public authority, whilst ensuring the public authority (including local authorities) 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.[2]

5. This Corporate RIPA & IPA Policy & Procedures Policy provides the Council guidance as to the use of covert surveillance and CD and has been approved by Cabinet.[3] In addition the Audit & Resources Committee has an oversight role and will therefore carry out high-level annual reviews of the RIPA & IPA Policy and Processes.

6. Any member of staff who is unsure regarding any aspect of this Policy and/or the statutory framework must contact the Council's Senior Responsible Officer[4] at the earliest opportunity.

7. **Compliance with this Policy and Procedures is mandatory for all relevant Council services and officers.** This Policy is accessible on the Council's Staff Hub.

## (2) COUNCIL POLICY STATEMENT

8. Eastleigh Borough Council (EBC) takes its statutory responsibilities seriously and will always act in accordance with the statutory framework including relevant Orders and Codes of Practice. Accordingly, the Senior Responsible Officer (SRO) is duly authorised by the Council to monitor, review, and amend this Policy as and when required. For administration and operational effectiveness, the SRO is also authorised to add or substitute an Authorising Officer or Designated Senior Officer when required.

[1] Article 8 ECHR
[2] Human Rights Act 1998 Section 6 – It is unlawful for a public authority to act in a way which is incompatible with a Convention right.
[3] 23-01-2023
[4] **Appendix 1**

## (3) RIPA STATUTORY FRAMEWORK

### 3.1 DEFINITION OF SURVEILLANCE

9. Surveillance for the purposes of RIPA includes [5]:

(a) monitoring, observing, or listening to persons, their movements, their conversations or their other activities or communications;

(b) recording anything monitored, observed, or listened to in the course of surveillance;

(c) surveillance by or with the assistance of a surveillance device;

10. 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 [6]:

(a) the communication is one sent by or intended for a person who has consented to the interception of communications sent by or to them; and

(b) there is no interception warrant authorising the interception.

11. Methods of "recording," surveillance were expanded in Part 2 of 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[7]. The Act states "surveillance camera systems include… any other systems for recording or viewing visual images for surveillance purposes,[8]" which includes Body Worn Videos, as confirmed by the College of Policing Body Worn Guidance 2014 and AB v Hampshire Constabulary IPT/17/191/CH [2019].

### 3.2 LAWFUL SURVEILLANCE

12. Surveillance will be lawful if[9]:

(a) an authorisation under this Part confers an entitlement to engage in that conduct on the person whose conduct it is; and

(b) his conduct is in accordance with the authorisation

### 3.3 TYPES OF SURVEILLANCE

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

[5] RIPA Section 48(2)(a)-(c)
[6] RIPA Section 48(4)
[7] First published June 2013, amended November 2021
[8] Protection of Freedoms Act 2012 Section 29(6)(b)
[9] RIPA Section 27(1)

**3.4 OVERT SURVEILLANCE**

14. 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.

**3.5 COVERT SURVEILLANCE**

15. 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.[10]

**3.6 CATEGORIES OF COVERT SURVEILLANCE**

16. There are three categories of covert surveillance:

**i) Directed**[11]
**ii) Covert Human Intelligence Source [CHIS]**[12]
**iii) Intrusive**[13]

**Please note, local authorities are prohibited from conducting intrusive surveillance.**

**3.7 DIRECTED SURVEILLANCE**

17. Directed surveillance (DS) is **covert** but not intrusive surveillance and undertaken[14]:

a) for the purposes of a **specific investigation** or a specific operation;

(b) 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

(c) 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** under this Part II to be sought for the carrying out of the surveillance.

Example

18. 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.

[10] RIPA Section 26(9)(a)
[11] RIPA Section 28
[12] RIPA Section 29
[13] RIPA Section 32
[14] Covert Surveillance & Property Interference Revised Code of Practice 2018, paragraph 3.1

19. DS is necessary for the prevention or detection of crime as it is suspected the target has invented and/or exaggerated his purported disabilities, thus the offence being investigated is fraud. Fraud is a criminal offence which satisfies the DS local authority pre-condition test, namely the Crime Threshold Test requiring the offence being investigated is punishable with imprisonment of at least six months (see below).

20. 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 is required and must be obtained along with Judicial Approval, before and in order, to ensure the DS is lawfully obtained and is any evidence obtained is admissible in criminal proceedings.

**3.8 COVERT HUMAN INTELLIGENCE SOURCES [CHIS]**

21. A CHIS is perhaps more commonly known as an informant. A person is a CHIS if they/them:[15]

a) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating that 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

22. 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.[16] A covert relationship and information obtained from it disclosed covertly, if and only if it is to be used, or as the cased 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.[17]

23. 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 assessed.

24. 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 such as where the incidental conduct is necessary to protect life and limb or national security.

[15] RIPA Section 26(8)(a)-(c)
[16] RIPA Section 26(9)(b)
[17] RIPA Section 26(9)(c)

**Key Difference Between Directed Surveillance & CHIS**

25. The key difference between DS and the use of a CHIS is that the first involves obtaining private information through covert means, whereas the second involves the manipulation of a relationship to obtain information. Any manipulation of a relationship amounts to a fundamental breach of trust which depending on the covert purposes, can place a CHIS in serious danger. Consequently, extra precautions may be required to ensure a CHIS is not identified.

**Establishing, Maintaining & Using a Relationship**

26. Establishing a relationship means the "set up," and maintenance of the relationship but which does not require endurance over any particular period[18] and so 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.

Example 1

27. 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 (see paragraph 39).

Example 2

28. 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/set up 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. Please note the additional safeguards for juvenile CHIS and the duration of the authorisation (see below).

**CHIS SCENARIOS**

29. A CHIS may be an officer or member of the public. Previous common examples of a CHIS were the infiltration of gang, or an undercover police officer recruited into a drugs operation.

**Relevant Source**

30. This is a CHIS who holds an office, rank or position with the public authority which does not include local authorities, hence they local authorities are **prohibited** from using this type of CHIS.[19]

[18] CHIS Draft Revised Code December 2021 paragraph 2.17
[19] Regulation of Investigatory Powers (Covert Human Intelligence Sources: Relevant Sources) Order 2013, Article 8

**Participating CHIS's**

31. The **Covert Human Intelligence Sources (Criminal Conduct) Act 2021**[20] introduced an explicit statutory power for the intelligence agencies, law enforcement and a number of limited wide public authorities to authorise a CHIS to participate in criminal conduct where it is necessary and proportionate to do so. Local authorities do not fall within the remit of wider public authorities and so are **prohibited** from utilising a participating CHIS.[21]

**Online Role Player**

32. 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 involving a tasked role player to establish and/or maintain a relationship for the covert purpose of obtaining information and/or provide access to any information to another person and/or the disclosure of information constitutes a CHIS, albeit the relationship is exclusively online.

33. The forums online role players can be deployed in include social media networking sites, chat rooms and online gaming Apps. Where a website or social media account requires a minimal level of interaction, such as sending or receiving a friend request before access is permitted, this may not be sufficient to amount to establishing a relationship. Equally electronic gestures such as "like," or "follow," in response to a post does not in itself constitute forming a relationship. Whilst these scenarios do not constitute a CHIS, they do both require a DS authorisation.

34. Some websites require a user to register providing personal identifiers such as name and phone number. If an officer is authorised to use a Council controlled account in a false identity (pseudonym) in order to register for a website, that in itself does not amount to establishing a relationship and so a CHIS authorisation is not immediately required. However, consideration should be given to the need for a directed surveillance authorisation if the conduct is likely to result in the acquisition of private information, and the other relevant criteria are met.

35. If an officer sends a request to join a closed group known to be administered by a subject of interest connected to a specific investigation a DS authorisation should be obtained to cover the covert monitoring of the site. If having entered the group it is intended the officer or CHIS will engage in such interaction to obtain, provide access to, or disclose information, a CHIS authorisation is required[22].
36. Where the use of the internet is part of the tasking of a CHIS, the risk assessment carried out in accordance with the Code,[23] 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.[24]

[20]The Regulation of Investigator Powers (Criminal Conduct Authorisations) (Amendment) Order 2021 (SI 2021/680) in force from 10 August 2021
[21] The Regulation of Investigator Powers (Criminal Conduct Authorisations) (Amendment) Order 2021, Article 7
[22] CHIS Draft Revised Code December 2021, paragraph 4.29
[23] CHIS Draft Revised Code December 2021, paragraph 4.31
[24] CHIS Draft Revised Code December 2021, paragraph 4.31

37. 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, providing clear information about the conduct required of each officer and including risk assessments in relation to each officer involved. This situation may arise when officers are working in shifts with regards their monitoring and interaction with the subject.

38. Please see below **ONLINE COVERT SURVEILLANCE INCLUDING SOCIAL MEDIA/NETWORKING SITES** for further guidance.

**Test Purchasing**

39. 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.

**Public Volunteer**

40. 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 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. However, please note this activity would require a DS authorisation[25].

41. If a person provides anonymous tip off information to a hotline, even if the caller obtained the information because of a relationship, such as reporting their son for having extensively graffitied a skate park located in Eastleigh, having seen the images on their son's private Instagram account, the parent is not a CHIS, as the information is not being disclosed on the basis of a relationship which was established or maintained for a covert purpose. However, if the caller is asked and agrees to be tasked to provide further information thereafter based upon their relationship, then a CHIS authorisation is required, and the informant should be treated as a CHIS.

**Status Drift**

42. A less obvious CHIS where a member of the public initially provides the information of their own volition and so was not tasked, but subsequently becomes a CHIS due to "status drift." This arises where the member of the public provides repeat information about suspect(s) in circumstances where it becomes apparent that the untasked informant obtained the information during his family or neighbourhood relationship. The reality is the untasked informant has due to status drift become an informant and thus is a CHIS.

[25] CHIS Draft Revised Code December 2021, paragraph 2.23

**Use of Equipment by a CHIS**

43. 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.

**Local Considerations & Community Impact Assessments**

44. For CHIS applications both 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 where an AO from a public authority considers that conflicts may arise, where possible 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.[26]

**SPECIAL CONSIDERATIONS FOR CHIS AUTHORISATIONS**

45. For both vulnerable individuals and juveniles, only the Chief Executive (Head of Paid Service) or the person acting as Chief Executive are permitted to authorise CHIS Applications and/or Renewals.[27] 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.[28]

**Vulnerable Individuals**

46. 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.[29]

[26] CHIS Draft Revised Code December 2021, paragraph 3.27
[27] CHIS Draft Revised Code December 2021, paragraph Annex A
[28] CHIS Draft Revised Code December 2021, paragraph 4.1
[29] CHIS Draft Revised Code December 2021, paragraph 4.2

**Juveniles**

47. 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[30]:

- Juvenile CHIS Authorisation duration extended from 1 to 4 months;
- Use of a Juvenile CHIS is not to be authorised unless the public authority has made a risk assessment which must take into account the risk of any physical injury or psychological distress to the source arising in the course of or as a result of the conduct being authorised. The assessment must be taken into account by the person granting the authorisation who must ensure any risks are justified and that the risks have been explained to and understood by the source. The risk assessment must be updated before any renewal is authorised;
- For sources between 16-18, a decision whether or not to inform a parent or guardian of a source is taken on a case by case basis;
- For sources under 16:

    - A prohibition on a source being tasked in relation to a parent or person with parental responsibility;

    - A requirement for an appropriate adult to be present at all meetings between the source and the public authority tasking them;

    - Requirement that where the young person's parent is available but may not themselves be suitable to act as one (e.g., if they support the ideology or criminal intentions of those against whom the juvenile CHIS may be deployed), there should be a suitable qualified person to act as the appropriate adult;

48. 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.

**MANAGEMENT OF A CHIS**

49. 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 Magistrate (Judicial Approval), must believe that in addition to the operation being necessary and proportionate, that arrangements exist ensuring that[31]:

(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."

[30] Regulation of Investigatory Powers (Juveniles) Order 2000 as amended by Regulation of Investigatory Powers (Juveniles) (Amendment) Order 2018 (SI 2018/715) and CHIS Draft Revised Code December 2021, paragraphs 4.3- 4.10

[31] RIPA Section 29(4A) & (5)

50. The handler of a CHIS will have day to day responsibility for dealing with and directing the CHIS, recording information supplied by the CHIS and monitoring the CHIS's security and welfare which should be brought to the attention of the CHIS controller if there are any concerns regarding the personal circumstances of the CHIS which might affect either the validity of the risk assessment; the conduct of the CHIS; and the safety and welfare of the CHIS. The handler is usually the rank or position below the AO.

(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;

(c) that there will at all times be a person of the specified rank with the relevant investigatory authority who will have responsibility for maintaining a **record** of the use made of the source;

(d) that the records relating to the source that are maintained by the relevant investigatory authority will always contain particulars of all such matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State;

(e) that the records maintained that disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons;

**CHIS Records**

51. Detailed records must be kept of the authorisation and use made of a CHIS in accordance with the Order.[32] In addition, records of copies of the following should be kept for at least five years[33]:

- a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer;
- a copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested;
- the reason why the person renewing an authorisation considered it necessary to do so;
- any authorisation which was granted or renewed orally (in an urgent case) and the reason why the case was considered urgent;
- any risk assessment made in relation to the CHIS;
- the circumstances in which tasks were given to the CHIS;
- the value of the CHIS to the investigating authority;
- a record of the results of any reviews of the authorisation;
- the reasons, if any, for not renewing an authorisation;
- the reasons for cancelling an authorisation; and
- the date and time when any instruction was given by the authorising officer that the conduct or use of a CHIS must cease.

[32] The Regulation of Investigatory Powers (Sources Records) Regulations 2000, Article 3 (a) – (n)
[33] CHIS Draft Revised Code December 2021, paragraph 8.1

52. Relevant investigatory authority," means the public authority for whose benefit the activities of that individual as such a source are undertaken.[34]

**Security & Welfare**

53. 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. Before authorising the use or conduct of a CHIS, the AO should ensure a risk assessment is carried out to determine the risk to the CHIS of any tasking and the likely consequences should the role of the CHIS become known. This should consider the risks relating to the specific tasking and circumstances of each authorisation and should be updated to reflect developments during the course of the deployment, as well as after deployed if contact is maintained. 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.

54. 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. For example, this could occur due to disclosure to a court or tribunal or any other circumstance where disclosure of information may be required and strategies minimising the risks to a CHIS or others should be put in place.

55. Where appropriate concerns about are raised to and considered by the AO, a decision must be taken as to whether or not the authorisation should continue.

**3.9 INTRUSIVE SURVEILLANCE**

56. As set out above, local authorities are **prohibited** from carrying out intrusive surveillance. Intrusive surveillance is covert surveillance that[35]:

a) consists in the carrying out of intrusive surveillance of any such description as is specified in the authorisation;

b) is carried out in relation to anything taking place on any residential premises or in any private vehicle;

c) is carried out for the purposes of, or in connection with the investigation or operation so specified or described

57. Intrusive surveillance involves the presence of an individual on the premises or in the 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.

[34] RIPA Section 29(8)
[35] RIPA Section 32(5)(a)-(c)

58. Private vehicle means any vehicle which issued primarily for the private purposes of the person who owns it or of a person otherwise having the right to use it.[36] Residential premises means so much of any premises as is for the time being occupied or used by any person, however temporarily, for residential purposes or otherwise as living accommodation (including hotel or prison accommodation that is so occupied or used). 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.[37]

**3.10 AERIEL COVERT SURVEILLANCE (DRONES)**

59. Where surveillance is to be carried out by airborne crafts or devices for example unmanned aircraft colloquially known as drones, consideration should be given as to whether a surveillance authorisation is required. In determining whether the surveillance is to be regarded as covert, consideration should be given as to the reduced visibility of a craft or device at altitude.

**3.11 ONLINE OVERT & COVERT SURVEILLANCE INCLUDING SOCIAL MEDIA/NETWORKING SITES**

60. Eastleigh Borough Council has published "Social Media Guidelines" which is found on the Staff Hub, and specially addresses the use of social media for investigations.

**Permitted Online Access**

61. 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,

**Prohibitions**

62. The following activity is **prohibited** by any Council staff member seeking to undertake either initial intelligence gathering and/or for any form of overt and/or covert surveillance.

**Officers are prohibited from:**

**(a) 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;**

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

**(c) 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;**

**(d) 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;**

[36] RIPA Section 48(1), S48(7)(a) - (b) & S48(8)
[37] The Regulation of Investigatory Powers (Extension of Authorisations Provisions: Legal Consultations) Order 2010 No 461

**ONLINE OVERT ACTIVITY**

**Publicly Available information (PAI)**

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

64. The fact the content of many social media sites and websites are freely accessible does not mean officers can access the material without 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.

65. Initially information accessed for intelligence purposes only and/or to establish or check basic facts are unlikely to require a DS RIPA authorisation. Further, if online open resource research is undertaken prior to an investigation, it is unlikely to engage privacy considerations and will not require a DS authorisation at that stage. Where a public authority has taken reasonable steps to inform the public or individual that the surveillance is or may be taking place, the activity is overt, and a DS authorisation is not normally required.

66. Undertaking open source research on platforms such as Companies House containing information about an individual in a publicly accessible database is unlikely to provide the subject a reasonable expectation of privacy. Similarly, subjects who post material on social media networks or websites to engage with a wide audience are less likely to hold a reasonable expectation of privacy in relation to that information.

67. Accessing social media accounts having been given full access with the consent of the owner does not negate the need to consider whether the account may contain information about others who have not given their consent such as friends who comment or post within this account, which constitutes collateral intrusion (see below).

**ONLINE COVERT ACTIVITY**

68. The use of a Council controlled account(s) to undertake online covert activity does not create a CHIS scenario, because it does not in itself amount to establishing a relationship, but consideration should be given to obtain a DS authorisation and Judicial Approval if the conduct is likely to result in the acquisition of private information and the other relevant criteria are met[38]. The key issue is therefore the intended purpose and scope the online activity is proposed to be.

[38] CHIS Draft Revised Code December 2021, paragraph 4.26

**Online Covert Directed Surveillance**

69. Factors to be considered in establishing whether a DS authorisation is required for online covert directed surveillance include[39]:

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

70. Where information is openly available in the public domain, whilst there may be a reduced expectation of privacy, such as where information relating to person or a group of people is made openly available within the public domain, there may still be privacy implications because whilst it was intended to make the information publicly available, it was not to be used for a covert purpose such as an investigation. This is the position regardless of whether a user of a website or social media platform sought to protect such information by restricting its access by activating privacy settings.[40]

71. An example would be a local Facebook buy and sell group with 5000 members for the purpose of offering new and/or used items for sale. 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.

72. Repeated or systematic viewing, collecting, or recording of private information from "open," social media sources such as Facebook, Twitter, Snapchat, and LinkedIn including information relating to the interests, activities and movements of individuals and their associates could be regarded as a form of 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 and the fact this information was provided and shared online does not alter this position.

[39] Covert Surveillance & Property Interference Revised Code of Practice 2018, paragraph 3.16
[40] Covert Surveillance & Property Interference Revised Code of Practice 2018, paragraph 3.13

73. Please note, internet searches carried out by third parties on behalf of a public authority may still require a DS authorisation.[41]

**Online Covert CHIS**

74. 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 such as e-messaging sites, in circumstances where the other parties could not reasonably be expected to know their true identity,[42] should consider whether the activity requires a CHIS authorisation.

75. 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.

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

**3.12 LOCAL AUTHORITY RIPA PROHIBITIONS**

**77. Local authorities are prohibited from carrying out:**

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

**78. 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.**

**3.13 LOCAL AUTHORITY RIPA LIMITATIONS**

79. RIPA limits local authorities to using three covert techniques for the purpose of preventing or detecting crime or preventing disorder[43]:

i) Directed Surveillance;
ii) Covert Human Intelligence Sources (CHIS);
iii) Communications data;

80. The Protection of Freedoms Act 2012 (POFA) came into force on 1 November 2012 and introduced significant changes and limitations to how local authorities are permitted to utilise RIPA, in addition to being required to obtain Judicial Approval (see below).

[41] Covert Surveillance & Property Interference Revised Code of Practice 2018, paragraph 4.32
[42] As an official rather than a private individual
[43] RIPA Schedule 1 Part 1 paragraph 17

**Judicial Approval of Local Authority RIPA authorisations**

81. 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.[44] Please note, Judicial Approval is no longer required for Communications Data applications (see below).

**Directed surveillance Crime Threshold Test**

82. 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[45]:

a) punishable whether on summary conviction or indictment by a maximum custodial sentence of six months or more; or
b) related to the underage sale of alcohol or tobacco;
c) related to underage sale[46] and/or proxy purchasing[47] of nicotine inhaling products[48]

83. Examples of offences that satisfy the Crime Threshold are more serious criminal damage, dangerous waste dumping and serious or serial benefit fraud. If an officer is unsure of the relevant criminal offence(s) being investigated or the penalties, legal advice should be obtained from a Prosecution specialist[49] who will assist in identifying the potential criminal offence(s) arising out of the facts of the investigation at that stage. 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.

**Prevention of Disorder**

84. Local authorities cannot authorise directed surveillance for the purpose of preventing disorder unless it involves criminal offence punishable by a maximum of term of at least 6 months e.g., affray which is normally prosecuted by the police in any event rather than a local authority. Local authorities are therefore no longer permitted to use RIPA for low level offences for example dog fouling, littering, dog control, fly posting. These restrictions therefore impact investigations from the outset as they require consideration at the commencement of an investigation as to whether the conduct being investigated is a criminal offence. If an investigation has already commenced for conduct amounting to a criminal offence that would satisfy the Crime Threshold test, but 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.

[44] Section 38 Protection of Freedoms Act 2012
[45] Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2012 (SI 2012/1500)
[46] Lawful age to sell nicotine inhaling products is 18
[47] The adult making the purchase commits the offence not the retailer
[48] The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) (Amendment) Order 2015 (SI 937) in force since 1 October 2015
[49] **Appendix 11**

### 3.14 TWO MANDATORY TEST FOR DIRECTED SURVEILLANCE & CHIS

#### 3.14.1 NECESSITY

85. A local authority Authorising Officer (AO) shall not grant an authorisation for the carrying out of Directed Surveillance and/or CHIS unless he/she believes the authorisation is **necessary**. The sole necessity ground applicable to local authorities is," **for the purpose of preventing or detecting crime or disorder**."[50]

86. 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).

#### 3.14.2 PROPORTIONALITY

87. A local authority Authorising Officer (AO) shall not grant an authorisation for the carrying out of Directed Surveillance and/or CHIS unless he/she believes the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.[51] No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means.

88. The following should be considered in determining proportionality:[52]

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

89. The officer completing and submitting the application must carefully explain why the particular covert method, technique and tactic is an appropriate use of RIPA and a reasonable way of achieving the desired objective.

90. The AO must consider the risk of obtaining private information about persons who are not the subjects of the surveillance (collateral intrusion). In brief, the AO needs to clearly articulate why the proposed activity is proportionate to what is sought to be achieved and take into account, the risk of obtaining private information about persons who are not the subjects of the surveillance activity (collateral intrusion). The AO's considerations need to be fully documented.

[50] RIPA Directed Surveillance Section 28(3)(b) & CHIS Section 29(3)(b)
[51] RIPA Directed Surveillance Section 28(2)(b) & CHIS Section 29(2)(b)
[52] Covert Surveillance & Property Interference Revised Code of Practice 2018, paragraph 4.7

### 3.15 AUTHORISATIONS

91. Surveillance will be lawful if[53]:

(c) an authorisation under this Part confers an entitlement to engage in that conduct on the person whose conduct it is; and

(d) his conduct is in accordance with the authorisation

## (4) KEY ROLES

### 4.1 AUTHORISING OFFICERS

92. A designated person known as an "Authorising Officer," (AO) is lawfully permitted to grant authorisations for Directed Surveillance or use of a CHIS. The rank of local (AO's) lawfully permitted to act as AO are ***Director, Head of Service, Service Manager or equivalent***.[54] EBC's list of AOs is contained within the Appendices[55] and is reviewed and maintained by the SRO. Before and in order to become an AO, training must be completed the SRO must authorise the AO to commence their role.

93. The Chief Executive is an AO's (Head of Paid Service) and is the only one permitted to approve any action or operation involving the recruitment of a juvenile CHIS, any other vulnerable person or where surveillance may result in the Council obtaining access to legally privileged or confidential information. Please note, local authority authorising officers are not permitted to authorise urgent authorisations.

94. AOs are responsible for ensuring all staff who report to them for the purposes of RIPA receive a copy of this Policy; are informed of the mandatory requirement to follow this Policy; require internal authorisation and thereafter Judicial Approval before a covert surveillance operation can be undertaken and commenced.

95. The Investigatory Powers Commissioners Officer (IPCO) confirms the "responsibility for authorising an activity always remains with the Authorising Officer," even after Judicial Approval. This responsibility includes conducting timely reviews, renewals if required and cancelling the authorisation promptly once the operation is concluded or if grounds for the authorisation no longer apply, rather than simply permitting the remaining time of the authorisation to run out.

96. All AOs should wherever possible be independent of the investigation and this is one of the criteria within the RIPA URN Request Form.[56] Where the AO authorises their own activity this will be recorded in the RIPA Centrally Retrievable Record[57] and should be highlighted to the IPCO inspector at the next inspection.

---

[53] RIPA Section 27(1)
[54] The Regulation of Investigatory Powers (Directed Surveillance and Covert Human Intelligence Sources) Order 2010 No 521, Schedule, Part 1 & 480
[55] **Appendix 2**
[56] **Appendix 15**
[57] **Appendix 5**

97. AOs are urged not, "restrict contemplation to the type of tactic rather than the specific facts of the activity. It is unwise to approach RIPA … from the perspective of labels." It is the AO's statutory duty to be satisfied the proposed activity is both necessary and proportionate. The AO should set out in their own words why they believe the covert surveillance is both necessary and proportionate.

98. AOs should routinely state "who, what, when, where and how," i.e., who is the target; what action is being authorised; when it is to take place; where or at which location; how the activity is to be done. Care must also be taken to ensure words used do not unintentionally limit the activity. This can be avoided by using wording such "and/or," to permit both alternatives.

99. AO's must also pay particular attention to Health and Safety issues that may arise or be raised by any propose surveillance. Under no circumstances should an AO approve a RIPA application any form of surveillance unless and until, they are health and safety of Council employees/agents are suitably addressed and/or the risks minimised, so far as is possible and proportionate to/with the proposed surveillance. If any AO is in any doubt, they should obtain prior guidance regarding the issue from a member of the Management Team, the Council's Health and Safety Officer and/or the SRO.

**4.2 SENIOR RESPONSIBLE OFFICER**

100. The Council's Senior Responsible Officer (SRO) is the Council's Legal Services Manager[58] in accordance with the requirement that the SRO is a member of the corporate leadership team[59]. The Codes for Directed Surveillance, CHIS and Communications Data specifies the SRO is responsible for[60]:

- The integrity of the process in place within the public authority to authorise directed surveillance and request communications data;
- Compliance with Part II of RIPA, Part 3 of Investigatory Powers Act (IPA) and Codes
- 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; similarly, to The Office of Communications Data Authorisations (OCDA)
- Engagement with IPCO and inspectors who support the Commissioner when they conduct their inspections; similarly, with OCDA and its inspectors;
- Where necessary, overseeing the implementation of any post-inspection action plans recommended or approved by a Judicial Commissioner; similarly, the Investigatory Powers Commissioner;
- Ensuring that all authorising officers are of an appropriate standard, addressing any recommendations and concerns in the inspection reports prepared by the Investigatory Powers Commissioner;

[58] **Appendix 1**

[59] Directed Surveillance & Property Interference Revised Code of Practice 2018, paragraph 4.46

[60] Directed Surveillance & Property Interference Revised Code of Practice 2018, paragraph 4.41

101. 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 to ensure they are aware of the RIPA statutory framework and process.

### 4.3 JUDICIAL APPROVAL

102. Since 1 November 2012 local authorities must obtain Judicial Approval for both Directed Surveillance and CHIS Applications and Renewals, in addition to requiring internal authorisation from an AO. Please note, Judicial Approval is not required for reviews or cancellations and is no longer required for Communications Data applications (see below). The process for applying for Judicial Approval is set out in **Appendices 18 & 19** and the authorisation does not commence until it has been obtained.

## (5) KEY TERMS

### 5.1 PRIVATE INFORMATION

103. 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,[61] 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. An example would be two people holding a conversation in a bus street or on a bus who may have a reasonable expectation of privacy over the contents of their conversation and so a DS authorisation would be appropriate for a public authority to record or listen to the conversation as part of a specific operation or investigation.

### 5.2 COLLATERAL INTRUSION

**Directed Surveillance**

104. Before authorising directed surveillance, the AO should consider the risk of obtaining private information about persons who are not the subjects of the surveillance. Particular consideration should be given in cases where religious, medical, journalistic, or legally privileged material may be involved or where communications between a member of parliament and another person on constituency business may be involved.

105. An application should include an assessment of the risk of collateral intrusion and the details of any/all measures taken to limit this, to enable the AO to fully consider the proportionality of the proposed actions, such as pixelating the faces of the children and/or partner of the target.

[61] RIPA section 26(10)

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

**CHIS**

107. 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. If collateral intrusion is unavoidable, the activities may still be authorised provided it is considered proportionate to the aims of the intended intrusion and it should be kept to a minimum necessary to achieve the objective of the operation. All applications should include an assessment of risk of any collateral intrusion and details of any measures taken to limit this, to enable the AO to fully consider the proportionality of the proposed use or conduct of a CHIS.

**5.3 CONFIDENTIAL OR PRIVILEGED MATERAIL**

108. Particular consideration should 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:

i) Confidential journalistic material or a journalist's source;
ii) Legally privileged;
iii) Confidential personal information or communications between an MP and another person or constituency business;

**Confidential Information**

109. Confidential information can include oral and written communications held in confidence concerned an individual (living or dead) who can be identified from it and the material in question relates to his/her physical or mental health or to spiritual counselling. The material therefore consists of personal information (such as medical records or spiritual counselling, confidential journalistic material, confidential discussions between Members of Parliament and their constituents) or matters subject to legal professional privilege (solicitor and client).

110. Directed surveillance likely to intended to result in the acquisition of knowledge of confidential or privileged material can only be granted by AO's permitted to grant authorisations for confidential or privileged information, namely the Chief Executive (Head of Paid Service) or the person acting as the Head of Paid Service.[62] Such information requires particular consideration and unwarranted access to them during an investigation may be grounds for cancelling the authorisation.

[62] Covert Surveillance & Property Interference Revised Codes of Practice 2018, Annex A

**Journalistic Material & Journalistic Sources**

111. 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 information being acquired for the purposes of journalism and held subject to such an undertaking.[63] Any authorisation seeking to acquire material that is believed will be confidential journalistic material must contain a statement that the purpose is to acquire material which is believed will contain confidential journalistic material. The AO must then consider what appropriate safeguards are required regarding the handling, retention, use and disclosure of the material.

112. A journalistic source is a person acting as an intermediary between the journalist and source. Any authorisation seeking to identify or confirm a source of journalistic information the authorisation must contain a statement that this is the purpose of the application, and the AO must then consider what appropriate safeguards are required regarding the handling, retention, use and disclosure of the material. Where confidential journalist material that identifies the source of the information is retained or disseminated to an outside body, the material should be marked "Confidential." Where such material has been obtained and retained for any other purposes, the matter should be reported to the Commissioner as soon as is reasonably practicable.

113. Where material is created or acquired with the intention of further a criminal purpose, the material is not to be regarded as having been created or acquired for the purposes of journalism.

**Items Subject to Legal Privilege**

114. 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 (right to a fair trial) as well as engaging Article 8. There are three scenarios where legally privileged items will or may be obtained:

i) Where privileged material is intentionally sought;
ii) Where privileged material is likely to be obtained; and
iii) Where the purpose or one of the purposes 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.

**Privileged Material Intentionally Sought**

115. This category of material includes the acquisition of such material during legal consultations which as set out above constitutes intrusive surveillance which local authorities are **prohibited** from doing (see above). Any application for such material outside of a legal consultation must contain a statement that the purpose or one of the purposes of the authorisation is to obtain legally privileged material and such an application should only be granted or approved if the AO be granted Judicial Approval as appropriate, is satisfied that there are exceptional and compelling circumstances that make the authorisation necessary where there is a threat to life or limb or in the interests of national security.

[63] Police Act 1997 Section 100

**Privileged Material Likely to be Obtained**

**116.** This category of material also includes the acquisition of such material during legal consultations which as set out above constitutes intrusive surveillance which local authorities are **prohibited** from doing (see above). Any application for such material outside of a legal consultation must be clear that the acquisition of such mattes is likely and should include reasons why the surveillance is necessary and an assessment of how likely it is that information subject to legal privilege will be obtained. The application should also confirm any inadvertently obtained material that is subject to legal privilege will be treated in accordance with the safeguards and that reasonable and appropriate steps will be taken to minimise access to the material that is subject to legal privilege.

**Covert Surveillance intended to result in the acquisition of knowledge of matters that would be subject to legal privilege if they were not created or held with the intention of furthering a criminal purpose**

117. This category of material also includes the acquisition of such material during legal consultations which as set out above constitutes intrusive surveillance which local authorities are **prohibited** from doing (see above). Any application in this scenario must include a statement setting out the reasons for believing that the items are likely to be created or held to further a criminal purpose e.g., communications with a lawyer seeking to obtain a false alibi or assisting the suspect in evading arrest will not be privileged as the communications are intended to further a criminal purpose. The Authorisation can only be issued where the AO and subsequent Magistrate consider the matters are likely to be created or held with the intention of furthering a criminal purpose.

**Covert Surveillance of Legal Consultations**

**118.** As set out above, 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. Local authorities are prohibited from undertaking any form of intrusive surveillance.

**Lawyers' Material**

119. Where a lawyer acting in their professional capacity is the subject of covert surveillance, it is possible that a substantial proportion of any material which will or could be acquired will be subject to legal privilege. Therefore, in any case where the subject of covert surveillance is known to be a lawyer acting in a professional capacity, the application should be made on the basis that it is likely or intended to acquire items subject to legal privilege and the procedure set out above must be followed.

## (6) KEY ADDITIONAL SURVEILLANCE ISSUES

### 6.1 ACTIVITY NOT FALLING WITHIN THE DEFINITION OF COVERT SURVEILANCE

120. 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 [64]and create and maintain written logs of activity which will be made available to internal and external oversight by IPCO.[65]

121. The Code of Practice on Covert Surveillance makes clear that routine patrols, observation at trouble "hotspots," immediate response to events and the overt use of CCTV are all techniques not requiring RIPA authorisation.[66]

122. 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:**

- Covert surveillance by way of an immediate response to events;
- Covert surveillance as part of general observation activities;
- Covert surveillance not relating to the statutory grounds in RIPA;
- Overt use of CCTV & ANPR systems;
- Certain other specific situations;

**Immediate Response**

123. Covert surveillance carried out as an immediate response to events so that it is not reasonably practicable to obtain a RIPA authorisation, does not require a DS authorisation even though it is likely to reveal private information about a person.[67]

**General Observation Activities**

124. 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. An example is EBC officers attending a car boot sale where it is suspected counterfeit goods are being sold. At that stage there is not a specific investigation and instead the intention is through reactive policy 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.

[64] **Appendix 26**
[65] Previously recommended by OSC's Procedures & Guidance 2016 (withdrawn by IPCO)
[66] Covert Surveillance & Property Interference Code of Practice paragraphs 2.21-2.29
[67] RIPA Section 26(2)(c)

**Surveillance not relating to specific grounds or core functions**

125. 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.

126. If a Council employee is suspected of undertaking additional employment during work hours, sick and holiday absences 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.[68]

127. 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 EBC, and the proposed DS is likely to result in obtaining private information. Accordingly, a DS authorisation should be considered and is required.

**Overt Surveillance Cameras – CCTV & ANPR**

128. The Council's overt CCTV is governed by Surveillance Camera Code of Practice and overseen by the Surveillance Camera Commissioner. The Code provides a framework of good practice including the processing of personal data[69] and a public authority's duty to comply with Human Rights Act 1998. Whilst the use of overt ANPR systems to monitor traffic flows or detect motoring offences does not require a RIPA authorisation, please note the Council's RIPA CCTV Protocol regarding third party requests for use of the Council's CCTV.[70]

129. "Surveillance camera systems," includes[71]

(a) CCTV & ANPR
(b) Any other systems for recording or viewing visual images for surveillance purposes
(c) Any systems for storing, receiving, transmitting, processing, or checking the images or information obtained by (a), (b); or
(d) Any other systems associated with, or otherwise connected with (a) – (c)

[68] C v The Police (IPT/03/32)
[69] Data Protection Act 2018
[70] **Appendix 25**
[71] Protection of Freedoms Act 2012 Section 29(6)

**Specific Situations – Authorisations Not Available**

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

- Use of a recording device by a CHIS for which a conduct authorisation permitted the recording of any information already exists;
- Overt or covert recording of the interview of a member of the public in a voluntary interview conducted by a public authority;
- 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;
- Entry on or interference with property or wireless telegraphy (not permitted by local authorities);

**6.2 COMBINED AUTHORISATIONS**

131. 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.

**6.3 COLLABORATION WITH OTHER AUTHORITIES/AGENCIES**

132. The Council will endeavour to obtain written collaboration agreements with any other authorities with whom it works regularly, such as the Police or neighbouring authorities.

**6.4 CCTV THIRD PARTY REQURESTS**

133. 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 RIPA CCTV Protocol.[72] 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 protocol are adhered to.

134. An example would be if the police requested to use the Council's overt CCTV cameras by diverting and directing them for a pre-planned specific investigation located at both entrances and within an alleyway situated off Upper Market Street, Eastleigh, as intelligence indicates there is a drug den operating in a vacant shop in Upper Market Street situated adjacent to the alleyway. 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, a DS authorisation application is not practicable and is therefore not required.

[72] **Appendix 25**

135. If any officer is in doubt as to how to proceed, please consult the Senior Responsible Officer at the earliest opportunity.[73]

**6.5 CONSEQUENCES OF NON-COMPLIANCE WITH RIPA**

136. 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:

**Evidence Rendered Inadmissible**

137. If covert surveillance is not lawfully undertaken the evidential product obtained may be deemed inadmissible by a trial judge in criminal proceedings,[74] as the court has the discretion to exclude evidence on which the prosecution proposes to rely to be given, if it appears to the court that, having regard to all the circumstances, including the circumstances in which was obtained, the admission of the evidence would have such an adverse effect on the fairness of the proceedings that the court ought not to admit it. Accordingly, the court may exclude the evidential product of covert surveillance because the prejudicial effect of adducing it outweighs any probative value.

**Legal Challenge**

138. Article 8 of the European Convention on Human Rights 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.

**Complaint to The Investigatory Powers Tribunal (**"IPT"**)**

139. This Tribunal is made up of senior members of the judiciary and the legal profession. Any person who believes that his or her Article 8 rights have been unlawfully breached by an authority using the RIPA authorisation process may submit a complaint the IPT.

[73] **Appendix 1**

[74] Police & Criminal Evidence Act 1984 Section 78

## (7) RIPA PROCESS

### 7.1 MANDATORY URN

140. 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 Council officer responsible for the RIPA Centrally Retrievable Register,[75] prior to the completion and/or submission of an application for DS or CHIS to an Authorising Officer (AO).

### 7.2 RIPA URN REQUEST FORM

141. Following the introduction of the Crime Threshold Test[76] the applicant/officer must answer the following six questions within the RIPA URN Request Form:[77]

i) Is DS/CHIS for the prevention or detection of Crime or disorder?

ii) If so, specify the criminal offence(s) being investigated and the statute(s);

iii) 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

iv) Does the offence(s) relate to the underage sale/supply of alcohol or tobacco/nicotine?

v) Is the proposed covert surveillance both necessary and proportionate?

vi) Have you considered collateral intrusion and how this could be minimised?

142. The completed RIPA URN Request Form must be emailed to the Officer responsible for the RIPA Centrally Retrievable Register or a prosecution specialist[78] in their absence. Once the RIPA URN Request Form is received, considered, and satisfied, an URN will be allocated from the electronic RIPA Central Retrievable Record of Authorisations kept and maintained by the relevant officer. All relevant information from this form must be inputted in the RIPA Centrally Retrievable Register and completed RIPA URN Request Form emailed to the applicant and named AO.

### 7.3 FORMS TO BE USED

143. All RIPA forms are to be accessed from the Home Office website to ensure all forms are the most recent version[79] and the link to the forms will also be located on the RIPA & IPA Staff Hub page.

---

[75] **Appendix 4**
[76] Protection of Freedoms Act 2012
[77] **Appendix 15**
[78] **Appendix 11**
[79] **Appendix 16**

**7.4 APPLICATION**

144. The application form should be submitted to an AO from the list of certified AOs.[80] The Applicant should ensure the Application sets out all relevant facts including providing details of the crime, proposed activity, and justification for the intended covert operation. 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.

145. 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[81]:

- All applications must set out 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;

**7.5 AUTHORISATION**

146. Officers must obtain both an internal authorisation of the application/renewal by an AO and Judicial Approval. The AO must be satisfied the authorisation or renewal is both necessary and proportionate and that in relation to directed surveillance, it also satisfies the Crime Threshold Test.

147. 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. Please note, the use or conduct of a source to obtain knowledge of matters subject to legal privilege MUST be subject to the prior approval of the Judicial Commissioner.

[80] **Appendix 2**

[81] Directed Surveillance & Property Interference Revised Codes of Practice 2018, paragraph 4.40

**7.6 JUDICIAL APPROVAL**

148. 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. The application and hearing process is contained in **Appendix 19**.

**Matters subject to Legal Privilege**

149. Where the activities of a CHIS will result in the CHIS obtaining, providing access to, or disclosing matters subject to legal privilege, EBC must obtain prior approval from an Investigatory Powers Judicial Commissioner before authorising such conduct. EBC must provide the Magistrate a copy of any such approval as part of the application process.

**Officers Authorised to Apply for Judicial Approval**

150. Eastleigh Borough Council has a list of authorised officers[82] who are lawfully permitted to appear on behalf of the Council to apply for Judicial Approval, rather than by an officer from Legal Services[83]. 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.

**Judicial Approval Application & Hearing Guidance**

151. To prepare for, attend and apply for Judicial Approval at West Hampshire Magistrates' Court, please follow the guidance contained in **Appendix 19.**

**Judicial Approval Process between EBC & West Hampshire Magistrates' Court**

152. To prepare for and arrange a Judicial Approval Application Hearing, please follow the Protocol contained in **Appendix 18.**

**Outcomes**

153. There are 3 possible outcomes for an Application for Judicial Approval:

i) Application Granted → effective from that date and time;

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

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

154. Please 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.

[82] **Appendix 7**
[83] Local Government Act 1972 Section 223

**DURATION**

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

- Directed Surveillance 3 months
- CHIS 12 months
- Juvenile CHIS 4 months[84] (see review requirements)

**REVIEWS**

156. 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 RIPA Centrally Retrievable Record (CRR).[85]

**Directed Surveillance**

157. 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.

158. 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.

159. Where the surveillance provides access to confidential information or involves collateral intrusion, the AO should conduct regular more frequent reviews. It is also possible and appropriate for an AO to cancel aspects of an authorisation during the course of a review where it is no longer required such as DS against one of a number of named subjects.

**CHIS**

160. 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 (if applicable). 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 (if applicable).

[84] Regulation of Investigatory Powers (Juveniles) (Amendment) Order 2018 (SI 2018/715). Duration increased from 1-4 months.

[85] **Appendix 5**

161. A juvenile CHIS authorisation is now 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.[86]

**RENEWALS**

162. Renewals are permitted more than once, and the fact and outcome should be recorded in the RIPA CRR. 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.

163. 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.

**CANCELLATION**

164. The officer has a duty to request the AO to cancel an 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.

165. 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.

166. 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 who must then update the RIPA CRR. 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.

**7.7 RIPA CENTRALLY RETRIEVABLE REGISTER**

167. The SRO is responsible for maintaining a RIPA Centrally Retrievable Register (CRR) which must include all the categories of data required by the Code.[87] From February 2022 the Council will use an electronic CRR to record the required details.[88] The previous RCRR paper version and thereafter electronic record must both be retained for perpetuity.

[86] CHIS Draft Revised Code December 2021, paragraph 5.20 & 7.17
[87] Directed Surveillance & Property Interference Revised Code 2018 paragraph 8.1
[88] **Appendix 5**

**7.8 RIPA DOCUMENTATION - CENTRALLY RETRIEVABLE RECORDS**

168. The SRO is also required to obtain and retain for all covert surveillance operations the following, in a restricted location[89]:

**i)** RIPA URN Request Form;
**ii)** All original applications, any supplemental documentation, and the authorisations;
**iii)** Copy of the granted Judicial Approval Form B; (Application/Renewal);
**iv)** Copy of the Order granting Judicial Approval (Application/Renewal);
**v)** A record of the period over which the surveillance has taken place;
**vi)** The frequency of reviews prescribed by the AO;
**vii)** A record of the result of each review;
**viii)** A copy of any renewal of an authorisation together with the supporting documentation submitted when the renewal was requested;
**ix)** The date and time when any instruction to cease surveillance was given;
**x)** The date and time when any other instruction was given by an AO;

169. 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[90] via the designated email address[91]. The Judicial Approval Applicant must similarly provide the SRO by hand the original Judicial Approval granted/refused Form B within **7 days** of grant in a sealed envelope marked "**Strictly Private & Confidential**," and/or email a scanned copy to the SRO via the designated email address.

**RETENTION OF RECORDS**

170. 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 where equitable to do so, may consider complaints made more than one year after the conduct to which the compliant relates, particularly where continuing conduct is alleged. 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 **five years**.

## (8) SAFEGUARDS

171. Public authorities should ensure their actions when handling information obtained by covert surveillance comply with relevant legal frameworks and the Code so that any interference with privacy is justified in accordance with ECHR Article 8(2). Compliance includes data protection to ensure the handling of private information obtained continues to be lawful, justified and strictly controlled and is subject to robust and effective safeguards. Any breach must be reported to the Commissioner and any breaches of data protection should be reported to the Information Commissioner. Public authorities must also keep their internal safeguards under periodic review to ensure they remain up to date and effective.

[89] Directed Surveillance & Property Interference Revised Code 2018 paragraph 8.2
[90] **Appendix 1**
[91] Headoflegal@eastleigh.gov.uk

**8.1 DISSEMINATION**

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

- is or is likely to become necessary for any of the statutory purposes set out in RIPA in relation to covert surveillance (the remaining provisions to do not apply to local authorities[92]);
- is necessary to facilitate the carrying out of the functions of the public authorities under RIPA;
- is necessary for facilitating the carrying out of any functions for the Commissioner of IPT;
- is necessary for the purposes of legal proceedings; or
- necessary for the performance of the functions of any person by or under any enactment

173. In addition to limiting the number of persons to whom the material should be disseminated to, 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.[93]

**8.2 USE OF MATERIAL AS EVIDENCE**

174. Subject to the statutory framework governing the admissibility of evidence[94] 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).

**8.3 HANDLING MATERIAL**

175. 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.

**8.4 COPYING**

176. 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).

[92] Police Act 1997 & Intelligence Services Act 1994

[93] Covert Surveillance & Property Interference Revised Code 2018 paragraph 9.6

[94] Criminal Procedure & Investigations Act 1996; Civil Procedure Rules, Police & Criminal Evidence Act 1984 section 78 and the Human Rights Act 1998 & Covert Surveillance & Property Interference Revised Code

**8.5 STORAGE**

177. 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. The following protect security measures must be applied to the material:

- material must be inaccessible to officers not connected to the operation;
- material must be inaccessible to officers connected to but not authorised by the Officer in Charge (OIC) of the investigation to have access;
- IT security to minimise the risk of unauthorized access to IT systems;

**8.6 DESTRUCTION**

178. 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) set out in paragraph … above.[95] If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying information means taking such steps as might be necessary to make access to the data impossible. 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.

**8.7 PROTECTION OF THE IDENTITY OF A CHIS**

179. CHIS's may place themselves at considerable risk, thus 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.

180. 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 in such circumstances or by abandoning the prosecution in order to protect the fact and identity of the CHIS. This would be dealt with by Legal Services and prosecution counsel in conjunction with the AO, as the Council would be the prosecuting authority.

[95] Covert Surveillance & Property Interference Revised Code 2018 paragraph 9.5

## (9) ACQUISITION OF COMMUNICATIONS DATA

181. The Investigatory Powers Act 2016 (IPA)[96] Part 3 and the Code of Practice[97] 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.[98]

### 9.1 OFFICE OF COMMUNICATIONS DATA AUTHORISATIONS (OCDA)

182. The Investigatory Powers Commissioner's Office is responsible for the independent authorisation of CD requests which is delegated to the Office of Communications Data Authorisations (OCDA).[99]

### 9.2 LAWFUL AQUISTION OF CD

183. IPCO may authorise a public authority to engage in any conduct which is[100]:

a) For the purpose of obtaining data from any person; and
b) Relates to:
   i) a telecommunications system, or
   ii) data derived from a telecommunications system

### 9.3 COMMUNICATIONS DATA

184. 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)[101]. Generally, CD is acquired from a Telecommunications Operator (TO) (previously referred to as the Communication Service Provider).

### 9.4 TWO CATEGORIES OF COMMUNICATIONS DATA (CD)

185. All communications data held by a telecommunications operator or that which is obtainable from a telecommunications system now falls into two categories of CD, replacing the three subcategories of CD under RIPA (subscriber data; traffic data; and service use information).

[96] In force since 11 March 2019
[97] Communications Data Code of Practice November 2018
[98] Investigatory Powers Act 2016 Section 73(1)
[99] Investigatory Powers Act 2016 Section 60A
[100] Investigatory Powers Act 2016 Section 60A (2)
[101] Communications Data Code of Practice November 2018, paragraph 2.18

## 9.5 ENTITY DATA

186. Entity data covers information about a person or thing and about links between a telecommunications service, part of a telecommunications system and a person or thing that identify or describe the person or thing. This therefore includes devices such as phones, tablets and computers and the link between a person and their device is the entity data.[102] This category of CD broadly replaces subscriber data and includes:

- Subscriber information — identify of the person to whom the services are provided
- Subscriber checks — who is the subscriber of the phone number 01234 567890
- Subscriber/account holder — names, address of installing, billing payments etc.
- Connection/disconnection Reconnection information — what the account holder is allocated or has subscribed to

## 9.6 EVENTS DATA

187. Events data identifies or describes events which consist of one or more entities engaging in an activity at any specific time or times. Event Data refers to both Traffic Data and Service Use Information. Events data includes the following details regarding the communication[103]:

- Date and time sent;
- Duration;
- Frequency;
- Call diversion;
- IP address;
- Information tracing the origin or destination of a communication that is or has been in transmission;
- Sender or recipient of a communication
- 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);
- Itemised telephone call records;
- Volume of data downloaded and/or uploaded;
- Use of services i.e., conference calling, call messaging, call waiting

## 9.7 LOCAL AUTHORITY PROHIBITIONS

**188. Local Authorities are prohibited from:**

**i) obtaining the content of any communication i.e., what was said or written;**
**ii) acquiring the Internet Connection Records (ICRs)**

[102] Communications Data Code of Practice November 2018, paragraph 2.38
[103] Communications Data Code of Practice November 2018, paragraph 2.45

## 9.8 TWO MANDATORY TESTS FOR COMMUNICATIONS DATA REQUESTS

### 9.8.1 NECESSITY

189. Local authorities as relevant public authorities are permitted to internally grant and seek external authorisation from NAFN and thereafter Office of Communications Data Authorisations (OCDA) for authorisations if and only if they are necessary[104] for the **applicable crime purpose**."[105]

**Applicable Crime Purpose**

190. The applicable crime purpose test was introduced on 1 November 2018[106] and the purpose depends on whether the CD being sought is entity or events data:[107]

(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 – Events Data**

191. Applications for CD which are wholly or partly events data are now[108] only permitted where they are necessary for the purpose of preventing or detecting serious crime**.** Applications for Entity Data must be necessary for the purpose of preventing or detecting crime or preventing disorder but do not have to constitute a serious crime.

192. Offences satisfying the Serious Crime Threshold are[109]:

- An offence capable of attracting a prison sentence of 12 months or more (for persons 18+ in England)
- An offence by a person who is not an individual (i.e., corporate body);
- An offence which involves, as an integral part of it, the sending of a communication;
- An offence which involves, as an integral part of it, a breach of a person's privacy;
- 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);

### 9.8.2 PROPORTIONALITY

193. The conduct the subject matter of the Application must be proportionate[110] to what is sought to be achieved.

[104] Investigatory Powers Act 2016 Section 61(1)(a)
[105] Investigatory Powers Act 2016 Section 60A(7)(b) introduced by The Data Retention & Acquisition Regulations 2018 Regulation 5
[106] The Data Retention & Acquisition Regulations 2018
[107] Investigatory Powers Act 2016 Section 60A (8)
[108] Since 1 November 2018
[109] Investigatory Powers Act 2016 Sections 86(2A) & 263(1)
[110] Investigatory Powers Act 2016 Section 61(1)(c)

## (10) KEY ROLES

### 10.1 SENIOR RESPONSIBLE OFFICER

194. The Council's Senior Responsible Officer (SRO) is the Council's Legal Services Manager.[111] The Communications Data Code of practice specifies the SRO is responsible for[112]:

- the integrity of the process in place within the public authority to acquire communications data;
- engagement with authorising officers in the Office for Communications Data Authorisations (where relevant); compliance with Part 3 of the Act and with this code, including responsibility for novel or contentious cases (see paragraph 8.45);
- 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;
- ensuring the overall quality of applications submitted to OCDA by the public authority;
- engagement with the IPC's inspectors when they conduct their inspections; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the IPC

### 10.2 DESIGNATED SENIOR OFFICER

195. 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,[113] which mirrors the rank required for RIPA AOs. The Council's DSOs are listed in **Appendix 3.**[114]

196. A DSO must be independent from those 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.

[111] **Appendix 1**
[112] Communications Data Code of Practice November 2018, paragraph 4.10
[113] Investigatory Powers Act 2016 section 73(2)
[114] **Appendix 3**

**10.3 NAFN SPOC & COUNCIL SPOC**

197. The SPOC facilitates the lawful acquisition of CD and effective cooperation between the public authority and OCDA and for local authorities, the required designated SPOC is NAFN. However, prior to submitting an application to NAFN, the Council's SPOC will assist the DSO and Applicant to provide advice regarding the following criteria, which mirrors NAFN's gatekeeping advice role once the Application is submitted:[115]

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

198. The SPOC must therefore be provided coverage for all CD acquisitions they intend to make. In exceptional cases where the SPOC is not available (sudden illness), public authorities should limit the risk by using collaboration arrangements with other authorities.[116] If this situation occurs, local authorities are expected to report to IPCO the circumstances and reasons requiring this course of action, prior to the next inspection.

**10.4 APPLICANT**

199. The applicant is a person involved in conducting or assisting an investigation/operation within a public authority who makes an application for the acquisition of communications data, which has to be done via NAFN for local authorities (see below).

[115] Investigatory Powers Act 2016 Section 76(5) & (6)
[116] Investigatory Powers Act 2016 Section 78

## (11) KEY TERMS

### 11.1 TELECOMMUNICATIONS OPERATOR

200. 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. This includes application and website provides but only if they provide a telecommunications service. This term replaces the previous term of Communications Service Provide (CSP).

### 11.2 CONTENT

201. 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.**

### 11.3 POSTAL OPERATOR

202. Postal service includes any service which consists of one or more of the collection, sorting, conveyance, distribution, and delivery of postal items and which is offered or provided as a service the main purpose of which, or one of the main purposes of which, is to transmit postal items from place to place. 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.

### 11.4 POSTAL DEFINITIONS

203. Communications data in relation to a postal service has 3 elements:[117]

i) *Postal data which is or has been compromised in or attached to the communication for the purpose of the service which it was transmitted*;

Includes any information that identifies or appears to identify any person or location to or from which a communication is or may be transmitted and includes addresses, markings on the outside of the postal item, records of correspondence, online tracking of communications.

*ii) Data relating to the use made by a person of a postal service;*

Includes information about the use made of services to which the user is allocated or has subscribed to, the price paid to send the item, records such as registered post etc

[117] Investigatory Powers Act 2016 section 262(3)(a) – (c)

*iii)* *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*

Includes information about any person to whom a service is provided, whether a subscriber or guest, if used or not used the service e.g., information about the person associated with a PO Box.

**11.5 INTERNET CONNECTION RECORDS (ICRs)**

204. An ICR provides details of the internet service that a specific device has connected to (e.g., a website or instant messaging application). It will not provide the full browser history of details of every web page visited, content or details of the recipient of a message or any activity on a particular website. **Please note local authorities are prohibited from obtaining ICRs.**

**11.6 THIRD PARTY DATA**

205. 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. The email provider will require the email address to route the communication but neither internet access provider has any need to see or access the full email address in order to connect the sender or recipient to the mail server.

206. Where one telecommunications operator 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 telecommunications operator is considered to process data if it specifically looks at an item of data in order to determine what action to take or if it has a set of rules in place which determine how a communication should be routed depending on certain items of data.

207. 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 telecommunications operator or postal operator 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.

**11.7 COLLATERAL INTRUSION**

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

### 11.8 JOURNALISTIC SOURCES

209. The only category of CD which requires local authorities to first obtain authorisation from OCDA 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.

### 11.9 NOVEL OR CONTENTIOUS CIRCUMSTANCES

210. 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 OCDA prior to progressing any conduct to acquire CD. This is a discretionary approach and if taken, a public authority must ensure the SRO is made aware and supports this course of action before the request for guidance to OCDA is submitted.

### 11.10 COLLABERATIVE ORGANISATION

211. An organisation that has formalised a collaboration agreement in place under the provisions of the Act, to be utilised for example where the SPOC is unexpectedly unavailable.

## (12) ACQUISITON OF COMMUNICATIONS DATA PROCESS

### 12.1 LOCAL AUTHORITIES

212. Local authorities are public authorities[118] who are permitted to acquire CD in limited circumstances but must be party to a collaboration agreement,[119] which requires their membership of **NAFN.**[120] IPA abolished the requirement for local authorities to obtain Judicial Approval for CD and since March 2019 local authorities **must** submit all CD Applications to NAFN for assessment as to whether the application should be submitted to The Office for Communications Data Authorisations (OCDA) to obtain authorisation.[121] Guidance as to the CD process is contained in **Appendix 24**.

### 12.2 OPERATIONAL PRIORITISATION

213. To assist OCDA as to the operational urgency of an application for CD and to ensure it is appropriately triaged, "Operational Prioritisation," was introduced. There are **four** prioritisation categories and **local authorities are only permitted** to use **Priorities 2-4**:

[118] Investigatory Powers Act 2016 Section 73(1)
[119] Investigatory Powers Act 2016 Section 73(1)
[120] National Anti-Fraud Network https://www.nafn.gov.uk/
[121] Commenced March 2019

| OPERATIONAL PRIORITISATION | DEFINITION |
|---|---|
| **Priority 1** | |
| **Immediate Threat to Life or Serious Harm** | **Not applicable to local authorities** |
| **Priority 2** | |
| **Urgent Operational Necessity** | 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 Constraint on Application)** | Not urgent but include specific or time critical issues such a 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** | 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 |

### 12.3 CATEGORY OF COMMUNICATIONS DATA REQUIRED

214. 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 victim reports receiving nuisance or threatening telephone calls or messages;
- a person who is the subject of an investigation or operation is identified from intelligence to be using a specific communications service;
- a victim, a witness or a person who is the subject of an investigation or operation has used a public payphone;
- a person who is the subject of an investigation or operation is identified during an investigation (such as a kidnap) or from detailed analysis of data available to the public authority to be using a specific communications service;
- 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); or
- a witness presents certain facts and there is a need to corroborate or research the veracity of those, such as to confirm the time of an incident they have witnessed.

**12.4 APPLICATION**

215. Officers should complete a Communications Data Application form within the NAFN website, ensuring it is clear as to whether the application is for Entity or Events Data; is necessary; satisfies the Applicable Crime Purpose test; and for Events Data also satisfies the Serious Crime Threshold Test. All Applications must also be proportionate and the Application to acquire CD must[122]:

- describe the communications data required, specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the data is required, by reference to a statutory purpose under the Act;
- include a unique reference number;
- include the name and the office, rank or position held by the person making the application;
- describe whether the communications data relates to a victim, a witness, a complainant, a suspect, next of kin, vulnerable person, or other person relevant to the investigation or operation;
- include the operation name (if applicable) to which the application relates;
- identify and explain the time scale within which the data is required;
- explain why the acquisition of that data is considered necessary and proportionate to what is sought to be achieved by acquiring it;
- 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;
- consider and, where appropriate, describe any meaningful collateral intrusion – the extent to which the rights of any individual not under investigation may be infringed and why that intrusion is justified in the circumstances;
- consider and, where appropriate, describe any possible unintended consequences of the application; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

216. General guidance for Applications is:

- All addresses should be accurately validated based on source material before the completion of the application form by both the Applicant and SPOC
- Keep all applications simple, legal, and concise;
- Avoid acronyms and abbreviations unless explained first;
- Use standard terminology to describe the main subject in your application (e.g., Victim, witness, complainant, suspect etc.);
- Clearly state the crime, offence, and purpose at the start of the Application;
- Be specific about daters of intelligence within the Application;
- Do not refer to another application, document, or system instead of addressing necessity and proportionality;
- 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;
- Clearly state the objective of your application. Do not name the services or products from the service provider;

[122] Communications Data Code of Practice November 2018, paragraph 5.4

- Ensure all applications are checked for accuracy of content and grammar before submission;
- 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;

**12.5 SPOC PROCESS**

217. Officers should inform their Service Manager prior to the completion of the application and before it is submitted to the CD SPOC. Once the application is complete it should be provided to the Council's CD SPOC[123] for review. The SPOC will as appropriate[124]:

- assess whether the acquisition of specific communications data from a telecommunications operator or postal operator is reasonably practicable or whether the specific data required is inextricably linked to other data; and
- advise applicants on the most appropriate methodology for acquisition of data where the data sought engages a number of telecommunications operators or postal operators;
- engage with applicants to develop and implement effective strategies to obtain communications data in support of operations or investigations;
- advise on and manage the use of the request filter, specifically in relation to progress of requests through the filter and compliance by the filter with the relevant authorisation (see chapter 11);
- advise on the interpretation of the Act, particularly whether an authorisation is appropriate;
- provide assurance that authorisations are lawful under the Act and free from errors;
- consider and, where appropriate, provide advice on possible unintended consequences of the application;
- assess any cost and resource implications to both the public authority and the telecommunications operator or postal operator of communications data requirements;

218. Where a number of providers are involved in the provision of a telecommunications service, consultation with the public authority's SPOC will determine the most appropriate plan for acquiring data and this will be set out in the application. It is the authorising individual who ultimately decides whether to authorise the acquisition of data.

219. If the SPOC is satisfied with the Application, the Applicant should submit it to the DSO for authorisation, but the DSO must also consult the SPOC before authorising it (see above). If authorised by the DSO the next stage is to submit the application to NAFN.

**12.6 DSO PROCESS**

220. 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:

- Objectively review the application;
- Objectively review an individual's right to privacy (not limited to the subject);
- Provide a bespoke authorisation avoiding use of standard phrases such as "the data should be held in accordance with the policy;
- Explicitly state the crime/offence you understand is the subject of the investigation;
- Clearly record have fully considered and understood the Application;

[123] **Appendix 10**

[124] Communications Data Code of Practice November 2018, paragraph 5.6

- Clearly record necessity is understood and has been considered;
- Clearly record proportionality is understood and has been considered;
- Clearly record consideration has been given to any potential for the authorisation to result in unintended consequences (e.g., collateral intrusion);
- Specifically state how the service requested will support the objective outlined in the Application;
- 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;
- 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

221. 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.

**12.7 SUBMISSION TO NAFN**

222. If the DSO authorises the Application, the officer must inform the SPOC and request the SPOC submit the application to NAFN, in accordance with the Communications Data Application Process Guidance (**Appendix 24**).

**12.8 OCDA'S REFUSAL TO GRANT AUTHORTISATION**

223. Where a request is refused by an authorising officer in OCDA, the public authority has three options:

i) not proceed with the request;

ii) resubmit the application with a revised justification and/or a revised course of conduct to acquire communications data;

iii) resubmit the application with the same justification and same course of conduct seeking a review of the decision by OCDA. A public authority may only resubmit an application on the same grounds to OCDA where the senior responsible officer or a person of equivalent grade in the public authority has agreed to this course of action. OCDA will provide guidance on its process for reviewing such decisions.

224. It is a matter for public authorities to decide what, if any, internal review mechanism exists for circumstances where a designated senior officer refuses to grant an authorisation. If NAFN refuse to submit the application to OCDA or OCDA refuses the Application for CD, the activity cannot commence

**12.9 AUTHORISATION**

225. An authorisation provides for persons within a public authority to engage in conduct relating to a postal service or telecommunication system, or to data derived from such a telecommunication system, to obtain communications data. The following types of conduct may be authorised:

- 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

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

226. An authorisation of conduct to acquire communications data may be appropriate where, for example:

- there is an agreement in place between a public authority and a telecommunications operator or postal operator to facilitate the secure and swift disclosure of communications data. Many telecommunications operators and postal operators have auditable acquisition systems in place to ensure accurate and timely acquisition of communications data, while maintaining security and an audit trail;

- where the data can be acquired directly from a telecommunication system and the activity does not constitute interception or equipment interference; or

- a public authority considers there is a requirement to identify a person to whom a service is provided but the specific telecommunications operator or postal operator has yet to be conclusively determined as the holder of the communications data.

227. An authorisation to give a notice may be appropriate where a telecommunications operator or postal operator is known to be capable of disclosing (and, where necessary, obtaining) the communications data. An authorisation of conduct to acquire communications data must[125]:

- describe the conduct which is authorised and describe the communications data to be acquired by that conduct specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the purpose for which the conduct is authorised, by reference to a statutory purpose under of the Act;
- include a unique reference number;
- specify the identity, rank, or position (or unique identifier) of the authorising individual granting the authorisation.
- where applicable, confirm in writing that a SPOC has been consulted on this application;
- record the date and, when appropriate to do so, the time when the authorisation was granted;
- specify when the communications data is to be obtained and disclosed by use of the request filter;

[125] Communications Data Code of Practice November 2018, paragraph 6.5

- if engaging the request filter, specify whether the processing of data (and its temporary retention for that purpose) is authorised and, if so, provide a description of the data that may be processed and the type or nature of processing to be performed (e.g., geographic correlation, IP address resolution);
- if engaging the request filter or acquiring ICRs, specify whether any threshold for the number of results returned is set which would prevent any portion of records being disclosed; and
- where data is being sought from a telecommunications operator or postal operator, specify whether the telecommunications operator or postal operator may inform the subject(s) of the fact that an application has been made for their data.

228. In addition, an authorisation to give a notice must[126]:

- specify the operator to whom the notice applies and the nature of requirements to be imposed;
- identify the public authority;
- Where the grant of an authorisation is recorded separately from the relevant application, they should be cross-referenced to each other.
- specify or describe the person(s) to whom the data is to be, or may be, disclosed or how to identify such person(s); and
- confirm whether a telecommunications operator or postal operator may disclose the existence of this requirement, or any related pursuant authorisation or notice, to a customer or other individual.

**12.10 NOTICES IN PURSUANCE OF AN AUTHORISATION**

229. The giving of a notice is appropriate where a telecommunications operator or postal operator 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 telecommunications operator or postal operator to obtain any communications data if that data is not already in its possession.

230. The decision to authorise the issuing of a notice must be based on information presented in an application. Once the authorising individual has authorised the giving of a notice, it will be given to a telecommunications operator or postal operator 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 notice must[127]:

- describe the communications data to be obtained or disclosed under the notice specifying, where relevant, any historic or future date(s) and, where appropriate, time period(s);
- specify the requirements being imposed and the telecommunications operator or postal operator on whom the requirements are being imposed;
- Ordinarily the applicant or other person within the investigation or operation will prepare a schedule of data, for example telephone numbers, to enable the SPOC to undertake the acquisition of subscriber information. The schedule will include details of the person who prepared it, cross reference it to the relevant notice or authorisation and specify the events data from which the data are derived

[126] Communications Data Code of Practice November 2018, paragraph 6.6
[127] Communications Data Code of Practice November 2018, paragraph 6.23

- specify the manner in which the data should be disclosed and specify or describe the person(s) to whom the data is to be, or may be, disclosed or how to identify such person(s);
- include a unique reference number and identify the public authority;
- specify the name (or unique identifier) of the officer giving the notice;
- be given in writing or, if not, in a manner that produces a record, within the public authority, of its having been given;
- record the date when the giving of a notice was authorised by the authorising individual;
- where appropriate, provide an indication of any urgency or time within which the telecommunications operator or postal operator is requested to comply with the requirements of the notice;
- include an explanation that compliance with the notice is a requirement of the Act unless the notice is cancelled. A telecommunications operator or postal operator which has not complied before the period of validity for the authorisation expires is still required to comply. The notice should contain sufficient information including the contact details of the SPOC to enable a telecommunications operator or postal operator to, where necessary, confirm the notice is authentic and lawful; and
- if permission has been given, confirm the telecommunications operator or postal operator may disclose the existence of this requirement, or any related pursuant authorisation or notice, to a customer or other individual

231. A telecommunications operator or postal operator 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 telecommunications operator or postal operator to disclose the communications data to the public authority. This will normally be to the public authority's SPOC.

**12.11 DURATION**

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

**12.12 RENEWAL**

233. 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 OCDA. Accordingly, the time required to complete this process must be factored in and back calculated from the current date of expiration, to ensure sufficient time is given in order to obtain a renewal authorisation from OCDA prior to the current authorisation expiring.

**12.13 CANCELLATIONS**

234. The DSO granting the authorisation must cancel it if at any time after the grant of authorisation by OCDA, 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.

**12.14 COMMUNICATIONS DATA CENTRALLY RETRIEVABLE RECORD**

235. The Council CD electronic centrally retrievable register is maintained by a Legal Services' Officer.[128]

[128] **Appendix 8**

**12.15 RECORD KEEPING**

236. 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.[129] Due to the degree of sensitivity and risk arising from obtaining and retaining documents in a central database, OCDA 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 OCDA. The Council has mirrored the retention period for covert surveillance documentation and will retain records for a period of 5 years.

237. Each relevant public authority must also keep a record of the following information[130](only those applicable to local authorities are listed):

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 OCDA;

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 OCDA;

F. the number of authorisations to give a notice to acquire communications data granted by the DSO and thereafter OCDA;

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);

[129] **Appendix 1**

[130] Communications Data Code of Practice 2018 paragraph 24.4

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 OCDA.

238. These records should distinguish between requests considered by OCDA[131] and those considered by designated senior officers.[132]

239. 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,[133] which is contained in the Council's Electronic Communications Data Centrally Retrievable Register (CRR).[134] If the advice of a Judicial Commissioner or OCDA has been sought prior to the acquisition of communications data that could be considered novel or contentious, the fact and views of OCDA 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.

## (13) SAFEGUARDS

### 13.1 GENERAL

240. 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[135] of Official with [136]a caveat of Sensitive, though it may be classified as higher if appropriate.

241. 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. Data must be effectively protected against unauthorised access and use, with particular consideration given to the principles of data security and integrity. Access to communications data must be limited to the minimum number of trained individuals necessary for the authorised purposes. Individuals should be granted access only where it is required to carry out their function in relation to one of the purposes for which the public authority may acquire communications data.

[131] Investigatory Powers Act 2016 Section 60A
[132] Investigatory Powers Act 2016 Sections 61 & 61A
[133] Communications Data Code of Practice 2018, paragraph 24.6
[134] **Appendix 9**
[135] Government Classification Scheme (2018)
https://security-guidance.service.justice.gov.uk/government-classification-scheme/#government-classification-scheme
[136] **Appendix 8**

242. The above 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[137]. 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. The CD CRR should be retained for perpetuity.

**13.2 RETENTION**

243. 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.

244. 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 where equitable to do so, may consider complaints made more than one year after the conduct to which the compliant relates, particularly where continuing conduct is alleged. 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 **five years**.

**13.3 NOTIFICATION**

245. Where communications data is being sought from a telecommunications operator or postal operator, if the telecommunications operator or postal operator 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).

**13.4 NOTIFICATION OF SERIOUS ERRORS**

246. 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.[138] 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.

[137] **Appendix 1**

[138] Investigatory Powers Act 2016 Section 231

### 13.5 NOTIFICATION IN CRIMINAL PROCEEDINGS

247. 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.

### 13.6 COMPLIANCE & OFFENCES

248. It is an offence for a person without lawful authority to knowingly or recklessly obtain CD from a telecommunications operator or postal operator.[139] It is a defence to show the person acted in the reasonable belief that the person had lawful authority to obtain the CD.[140] The offence is triable either way and is punishable in the Magistrates' Court with a maximum term of 12 months imprisonment and a maximum of two years in the Crown Court.[141]

## (14) DISCLOSURE DUTIES & OBLIGATIONS (RIPA & IPA)

249. In addition to considering document storage, retention and destruction, officers must also consider their Disclosure Duties & Obligations. The statutory framework for disclosure is Criminal Procedure & Investigations Act 1996, Criminal Procedure & Investigations Act Code of Practice,[142]Covert Surveillance & Property Interference Revised Code 2018,[143] CHIS Draft Revised Code December 2021 and Communications Data Revised Code of Practice 2018.

250. There is a duty to record, retain and review material created and/or obtained during an investigation. The Disclosure Officer (DO) is responsible for disclosure within the investigation, their disclosure obligations begin at the start of the investigation, and it remains a continuing duty to conduct a thorough investigation and manage all material appropriately. There is also a duty to follow all reasonable lines of inquiry whether they point towards or away from a suspect.

251. Unused material is material that is **relevant** but does not form part of the prosecution case. Relevant material **is *anything that appears to have some bearing on any offence under investigation, or any person being investigated, or on the surrounding circumstances unless it is capable of having an impact on the case*.**

[139] Investigatory Powers Act 2016 Section 11(1)
[140] Investigatory Powers Act 2016 Section 11(3)
[141] Investigatory Powers Act 2016 Section 11(4)
[142] Last revised 2015
[143] Chapter 9

252. The DO has a duty to review unused material and compile Disclosure Schedules containing Unused Material. There are two types of Schedules of Unused Material, firstly a Schedule of Non-Sensitive Unused Material[144] which is disclosable to the defence and must be provided to the defence either as part of Initial Disclosure and thereafter subsequent schedules or updates provided to the defence. The second is the Schedule of **Sensitive** Unused Material,[145] which is not disclosable to the defence due to its contents.

253. In compiling the schedules, the DO must assess each item to determine if it meets the **Disclosure Test**. The Disclosure Test requires the prosecution to provide the defence copies or access to any material which might reasonably be considered capable of undermining the prosecution case and/or assisting the defence, which has not been previously disclosed.

254. RIPA & CD Authorisations, Reviews, Renewal and Cancellation forms are usually listed in the Schedule of **Sensitive** Material as they are likely to disclose the systems and practices of the investigating authority. Directed Surveillance logs are usually listed in the Non-Sensitive Schedule albeit they may require redactions.

255. Once provided the relevant Schedules of Unused Material, the prosecutor has a duty to review the schedules and relevant documents, in particular the authorisation and supporting documents. If it is determined the material does not assist the defence or undermine the prosecution case, there is no requirement to disclose the material to the defence. Therefore, the Directed Surveillance or CHIS authorisation should only be disclosed to the defence (redacted if required) where it satisfies the disclosure test, or the defence has raised lawfulness of the authority.

256. R v GS & Others,[146] confirmed the validity or otherwise of surveillance authorisations goes to the lawfulness of the evidence obtained, not admissibility as Surveillance Commissioner's decisions, "shall not be subject to appeal or liable to be questioned in any court."

## 15. RIPA & IPA OVERSIGHT

### 15.1 APPROVAL OF POLICY

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

### 15.2 ANNUAL REVIEW OF POLICY

258. The Code[147] requires a review of the Policy at least once a year. The officer responsible for maintaining the RIPA Centrally Retrievable Record (CRR)[148] is also 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.

---

[144] Form MG6C
[145] Form MG6D
[146] [2005] EWCA Crim
[147] Directed Surveillance & Property Interference Revised Code 2018, paragraph 4.47
[148] **Appendix 5**

259. 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 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.

**15.3 RIPA & IPA BI-ANNUAL MEETINGS**

260. The introduction of RIPA and IPA bi-annual meetings chaired by the SRO for all those with designated roles will ensure all relevant updates to the statutory framework and any issues which arise from the SRO's internal monitoring of the RIPA Centrally Retrievable Record will be addressed and remedied where required in a timely manner. As set out above the SRO will prepare and submit an internal report to the elected members following the biannual meeting.

**15.4 INTERNAL MONITORING**

261. 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.

**15.5 TRAINING**

262. 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. The Council now has an electronic Central RIPA Training Register to record all RIPA training for AOs, DSOs officers and lawyers.[149] 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.

**15.6 REPORTING TO THE COMMISSIONER**

**Reporting Errors**

263. Public authorities are expected to have thorough procedures in place to comply with RIPA, for example the careful preparation and checking of authorisations to reduce the scope for making errors. A person holding a senior position within each public authority must undertake regular reviews of errors and a written record must be made of each review. This will be undertaken by the SRO.

264. An error must be reported it is a "relevant error,"[150] is an 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.

[149] **Appendix 21**

[150] Investigatory Powers Act 2016 section 231(9)

265. 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.[151] 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.

**Serious Errors**

266. IPCO is under a statutory duty[152] 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.[153]

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

267. The Commissioner must seek submissions from the public authority before deciding whether to inform the person regarding the error. If the Commissioner decides to inform the person of a serious error, the information provided to the person must include their right to apply to IPT and provide such details of the error as the Commissioner considers to be necessary for the exercise of those rights.

**15.7 CODES OF PRACTICE**

268. The Home Office publishes Codes of Practice for Covert Surveillance & Property Interference; CHIS; Communications Data and the Surveillance Camera, the links for which are contained in **Appendices**[154] and are located on the RIPA & IPA Staff Hub page and are admissible in evidence in any court proceedings. 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[155].

[151] Investigatory Powers Act 2016 Section 235(6)
[152] Investigatory Powers Act 2016 section 231
[153] Covert Surveillance & Property Interference Revised Code 2018 paragraph 8.16
[154] **RIPA COP Appendix 14 & IPA COP Appendix 20**
[155] **Appendix 1**

## 15.8 INVESTIGATORY POWERS COMMISSIONER'S OFFICE (IPCO)

269. The Investigatory Powers Commissioner's Office (IPCO) is the supervisory body for RIPA & IPA and deals with the following:

- Requests for RIPA Statistical Information;
- Inspections of Local Authorities usually every 2-3 years;
- Publication of regular reports on RIPA Activity;

## 15.9 INVESTIGATORY POWERS TRIBUNAL (IPT)

270. The IPT is an independent body with full powers to investigate and decide any case within its jurisdiction. The Tribunal has at its disposal a range of possible remedies, as wide as those available to an ordinary court which is hearing and deciding an ordinary action for the infringement of private law rights. The IPT will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates[156] particularly where continuing conduct is alleged.

271. Apart from compensation, other orders that may be made by the Tribunal include:

- an order quashing or cancelling any warrant or authorisation; and
- an order requiring the destruction of any records of information which (i) have been obtained in exercise of any power conferred by a warrant or authorisation; or (ii) are held by any public authority in relation to any person.

272. Any action unlawful covert surveillance or the acquisition of CD may have financial and reputational implications for the Council as well as affect its ability to utilise RIPA (see Gary Davies v British Transport Police (IPT/17/93/H)).

273. As to costs, unlike Rule 10 of the Tribunal Procedure (First-Tier Tribunal) General Regulatory Chamber Rules 2009 (SI No.1976) there is no express power to award costs in Section 67(7) of RIPA, nor in the Rules. The Tribunal has only awarded costs on one occasion (Chatwani & Others v the National Crime Agency).

[156] see section 67(5) of the Act