COVERT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES POLICY AND PROCEDURE MANUAL

Issue Date: January 2022

Covert Surveillance and Covert Human Intelligence Sources [CHIS] and Communications Data - Policy and Procedures

Contents

APPENDICES

Directed Surveillance & CHIS

1 Introduction

1.1 This Manual summarises the law for Local Authorities, and sets out the Council's policies, and procedure for three key types of surveillance activity. It draws on the latest Home Office Codes of Practice regarding the use of Covert Surveillance, and Covert Human Intelligence Sources [CHIS]. It also contains information about how and where to deal with any Communications Data issues, which, as a matter of Council policy and practice are now outsourced by the Council to the National Anti-Fraud network ("NAFN") via Trading Standards.

1.2 The application of the procedures in this Manual is mandatory for all Council service areas that undertake these functions. Historically these have been those dealing with Trading Standards, Housing, Social Services, Streetcare, and Audit & Investigations. In the past few years only Trading Standards have been regular users of RIPA powers, but it is essential all potential users are fully aware of this Manual's contents.

1.3 The Manual has been drafted based upon current legislation namely Regulation of Investigatory Powers Act 2000 Part II ["RIPA"], the Protection of Freedoms Act 2012 ("PFA"), and relevant Statutory Instruments. It refers to the Home Office Covert Surveillance and Property Interference Code of Practice, and the Home Office Covert Human Intelligence Sources Code of Practice, both made pursuant to section 71 RIPA and last updated and published in August 2018.

1.4 Where applicable and potentially helpful, relevant statutory provisions are referred to, so as to assist you in the application of the policies and procedures.

2 Definition of Surveillance

2.1 Surveillance for the purpose of RIPA includes: "monitoring, observing or listening to persons, their movements, conversations or other activities and communications". It may be conducted with (or without) the assistance of a surveillance device, and includes the recording of any information obtained. Surveillance can be undertaken whilst on foot, mobile or static.

2.2 This policy only relates to surveillance which is necessary on the grounds specified in the 2000 Act (specified at S28(3)) for directed surveillance. Covert surveillance for any other general purpose should be conducted under other legislation, if relevant, and an authorisation under this policy should not be sought.

2.3 Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognising that there may be an expectation of privacy over information which is on the internet, particularly when accessing information on social media websites.

3 Covert Surveillance

3.1 Surveillance is covert if and only if, it is carried out in a manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is (or may be) taking place [Section 26(9)(a)].

3.2 It must be likely to result in the obtaining of "private information" about the person observed. "Private Information" covers any aspect of a person's private or family life, including their family, professional and business relationships. Obviously it covers personal data like names, address and telephone, [Section 26 (10)], which are also covered by the GDPR and the DPA 2018.

3.3 This may happen in a public place where the person has a reasonable expectation of privacy whilst there, especially where:

a) the public authority concerned records the information gained, or
b) several records are to be analysed together to show a pattern of behaviour.

3.4 Surveillance of publicly accessible areas of the internet should be treated in a similar way, recognizing that there may be an expectation or privacy over information which is on the internet, particularly when accessing information on social media websites.

4 Types of Covert Surveillance

4.1 Covert surveillance may be: “Intrusive” or “Directed”.

Intrusive Surveillance

4.2 Local Authorities are NOT permitted to conduct Intrusive Surveillance at all. This covers anything taking place on/in any residential premises or a private vehicle, involving a person on the premises or in the car, [or using a device from outside that will produce images of the same quality as if they were inside like zoom lenses].

Directed Surveillance – with new limitations

4.3 Directed Surveillance must be:

- for the purpose of a specific operation or investigation (relating to a statutory enforcement function);
- its target must be unaware that it is or could be taking place;
- it must be done in a way likely to obtain private information about the target;
- it must not be an immediate response to events.

4.4 Local Authorities can now ONLY conduct Directed Surveillance for the Prevention or detection of crime. There is a minimum crime threshold so that offences must be punishable (whether on indictment or summary conviction) by a maximum term of 6 months imprisonment, or be related to the underage sale/supply of alcohol or tobacco/nicotine.

4.5 Note the minimum crime threshold does **not** apply to the use of CHIS.

5 Basis for lawful surveillance activity

5.1 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 of the rights are absolute, whilst others are qualified, meaning that it is permissible for the state to interfere with those rights provided certain conditions are satisfied. One of the qualified rights is the Right to respect for one’s private and family life, home and correspondence [Article 8 ECHR].

5.2 In limited circumstances Local Authorities are permitted to conduct Covert Surveillance, namely Directed Surveillance, and to use Covert Human Intelligence Sources [CHIS], both of which would result in the subject’s Article 8 Rights being infringed or interfered with by a public authority.

5.3 RIPA Part II (as amended by Regulations and the Protection of Freedoms Act 2012) provides the statutory framework to enable covert surveillance to be lawfully authorised and conducted - so as to ensure it is does not infringe the Article 8 rights, except as may be permitted by Article 8 (2), and to ensure the Council as a public authority is acting in a way compatible with the ECHR, as required by HRA section 6.

5.4 Since RIPA 2000 was passed and particularly since 2010, local authorities' powers have been increasingly curtailed. The additional purposes of protection of public health or in the interests of public safety, and the prevention of public disorder were removed.

5.5 To be sure a matter is RIPA controlled, officers must identify from the outset whether:
a) s/he is investigating a criminal offence - and if so,
b) whether it passes the 'threshold tests'.

5.6 From 1 October 2015 the 2010 Regulations were amended further - to add that the potential offence/s may relate to the purchase of alcohol on behalf of those under 18 (proxy purchases), or the sale of nicotine products to those under 18.

5.7 If an officer is unsure what specific criminal offence[s] are being investigated, or the penalties for them, legal advice should be taken from a Prosecution Lawyer, (see Appendix 3) who will identify any criminal offences arising out of the facts of the investigation at that stage. If no offence is identified, Directed Surveillance will not be permitted, but see also below.

5.8 Before proceeding with an application for the authorisation of Directed Surveillance, an applicant officer must also consider whether the proposed action is proportionate (as well as necessary) to prevent or detect crime above the threshold. Proportionality is discussed in paragraph 13 below, as it applies also to any proposal to use a CHIS.

5.9 Directed Surveillance cannot be used by local authorities to investigate low level offences such as littering, dog fouling and fly-posting, but there may be cases where the offence causing concern fails to pass the minimum RIPA crime threshold, but officers wish to take action to carry out their duties and protect local residents from harm to their social, economic or environmental well-being.

5.10 To avoid exposing the Council to the risk of reputational harm, or damages or costs, officers should seek advice as to whether it may be possible to satisfy the requirements of ECHR Article 8 (2) by alternative means.

5.11 The effect of RIPA section 80 is to make authorised surveillance lawful, but it does not make unauthorised surveillance unlawful. The Council reserves its right to exercise individual discretion, if presented with facts that justify an alternative view or approach, where a case lies outside the ambit of the RIPA regime and controls.

5.12 In such cases, the Council will work in line with its developing policy on non-RIPA surveillance and keep appropriate written logs of activity open to scrutiny by the SRO as recommended in Note 80 in IPC 2016 Guidance and Procedures.

6 Directed Surveillance Example

6.1 An example of Directed Surveillance is a covert static post e.g. an officer in car outside an address with a camera, to take pictures and/or follow of the target who has claimed Direct Payment, on the basis that s/he is severely disabled to the extent that s/he

cannot walk unaided and/or drive - but where it is alleged that the disabilities are invented and/or exaggerated.

6.2 The surveillance scenario would be covert, being used for a specific investigation and conducted in a manner likely to result in the obtaining of private information about a person (namely their movements/mobility in and around their home address and their daily activities), by video and/or photographic evidence. This operation is a clear example of Directed Surveillance.

7 Communications' Data

7.1 As a matter of policy and practice, the Council's Communications Data activities have been outsourced to the National Anti-Fraud Network ("NAFN") after a recommendation on a previous inspection. This is accessed via the Council's Designated Person whose details appear in Appendix 4.

7.2 The Council's SRO for these purposes is the same person as for the other RIPA activities, and their details appear in Appendix 1.

7.3 The Designated Person maintains a separate electronic register from the Council's Centrally Retrievable Records, subject to inspection and procedures in the Communications Data Code of Practice and related legislation.

7.4 Any staff considering the use of communications interception or other activity should refer initially to the Trading Standard's Work Instruction October 2013 [NAFN and Judicial Approval] which is set out in Appendix 5.

7.5 The Data Retention and Acquisition Regulations 2018 (SI 2018/1123) ("DRAR") have been in force since 1st November 2018 and amend Parts 3 and 4 of the Investigatory Powers Act 2016 which provide for the retention of communications data by telecommunications and postal operators, and the acquisition of that communications data by public authorities.

7.6 DRAR has introduced a new code of practice entitled "Communications Data" about the exercise of functions conferred by Parts 3 and 4 of the IPA (Reg 2).

7.7 Access to certain communications data (traffic or location data) may be authorized only for the prevention or detection of serious crime (Reg 3).

7.8 Independent authorisation of requests by public authorities to access communications data is now conferred on the Investigatory Powers Commissioner (Reg 5).

7.9 The power to access communications data is only exercisable if (Reg 6):

- In the interests of national security, or of the economic wellbeing of the UK so far as relevant to national security; or
- For the prevention or detection of serious crime.

8 Covert Human Intelligence Sources [CHIS]

8.1 A CHIS is perhaps more commonly called an "informant". A person is a CHIS if s/he:-

a) Establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within paras (b) or (c); and

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

8.2 The key difference between Directed Surveillance and use of a CHIS is that the first involves the obtaining of private information through covert means, whereas the second involves the manipulation of a relationship to obtain information. As an obvious breach of trust fundamental to personal relationships, this can pose serious danger to the CHIS if it is discovered.

8.3 In order to grant an authorisation for using a CHIS, the AO, and subsequently a Magistrate, must believe that in addition to the operation being necessary, and proportionate, that:

"arrangements exist for the source's case that satisfy the requirements of subsection (5) and such other requirements as may be imposed by order of the Secretary of State," [RIPA 2000, S29(2)(c)]

8.4 "Control" of a CHIS. Subsection (5) requires the CHIS to have:-

a) A "handler" of the specified rank with the relevant investigating authority, with day to day responsibility for the source

b) A "controller" of the specified rank with the relevant investigating authority with the general oversight of the use made of the source

c) That the records maintained that disclose the identity of the source will <u>not</u> be available to persons except to the extent that there is a need for access to them to be made available to those persons

d) "Relevant investigating authority," means the public authority <u>for whose benefit</u> the activities of that individual as such a source are to be undertaken. (NB: The Council occasionally undertakes joint operations.)

9 <u>Becoming a CHIS and 'status drift'</u>

9.1 A CHIS may be a member of the public or an officer acting with authority to do so. Common uses of CHIS are the infiltration of a gang e.g. football gangs or an undercover police officer being recruited into a drugs operation/conspiracy.

9.2 Please note that there may be circumstances where a less obvious CHIS exists. Care must be taken to identify that this person is a CHIS, and thereafter follow the correct procedure. An example is where a member of the public has given information, albeit not tasked to do anything with it. Such a person may be a CHIS if the information that s/he has covertly passed to LBR has been obtained in the course of (or as a consequence of the existence of) a personal or other relationship.

9.3 Although not specifically recruited to be a CHIS, such a person <u>may become</u> one. This situation is referred to by the IPC Procedures & Guidance 2016 as the risk of "status drift." Therefore, when an informant gives repeat information about a suspect or about a family, and it becomes apparent that the informant may be obtaining that information in the course of a family or neighbourhood relationship, it is a strong indication that the

informant is in reality a CHIS - to whom a duty of care is owed - if the information is then used. Legal advice must always be taken before using or acting on information received in these circumstances.

9.4 Becoming a CHIS gives rise to a duty of care owed to that person by the Council who seeks to benefit from their activity, as set out in paragraphs 8.2 and 8.3 above.

9.5 Trading Standards regularly undertake covert test purchasing, and task children to request a one-off sale. The Council, in accordance with IPC Guidance, takes the view that such conduct does not constitute a CHIS, as the child does not form any relationship with the target in a one-off sale. However you must consider whether covert test purchasing requires a Directed Surveillance authorisation.

9.6 Please note all authorisations for a juvenile CHIS or where confidential information may be obtained MUST be approved by the Chief Executive as Head of Paid Service. The Council must ensure that an appropriate adult is present at any meetings with a CHIS under 16 years of age. The appropriate adult should normally be the parent or guardian of the CHIS.

9.7 Trading Standards operate policy and procedures based on guidance from their national body.

9.8 The use and wearing of recording devices is done in accordance with the College of Policing Body Worn Video Guidance 2014.

9.9 It may be necessary to deploy covert surveillance against a potential or authorised CHIS, other than those acting in the capacity of an undercover operative, as part of the process of assessing their suitability for recruitment, deployment or in planning how best to make the approach to them. Covert surveillance in such circumstances may or may not be necessary on one of the statutory grounds on which directed surveillance authorisations can be granted, depending on the facts of the case. Whether or not a directed surveillance authorisation is available, any such surveillance must be justifiable under Article 8(2) of the ECHR

10 Requirement to obtain a URN from Principal Solicitor and Deputy Head of Litigation

10.1 For Directed Surveillance which satisfies the Crime Threshold Test or for a CHIS, the officer must first obtain a Unique Reference Number [URN] for the operation from a Principal Solicitor and Deputy Head of Litigation prior to the completion and/or submission of an Application for Directed Surveillance and/or CHIS to an AO.

10.2 In view of current requirements, the applicant must now answer the following 6 questions within the RIPA Request Form:-

i) Is DS/CHIS for the Prevention or Detection of Crime?
ii) Specify the criminal offence[s] being investigated and the statute[s]
iii) For Directed Surveillance only, does the criminal offence[s] meet the Crime Threshold Test (at least the 6 months maximum sentence); **or**
iv) Is the offence[s] for underage sale/supply of alcohol or tobacco/nicotine?
v) (For DS and CHIS) Is the action proposed both necessary and proportionate?
vi) Have you considered alternatives, who else could be subject to any collateral intrusion and how this could be minimised?

10.3 On receipt of the RIPA URN Request Form, the Principal Solicitor and Deputy Head of Litigation will consider the contents; allocate an URN from the electronic Central

Retrievable Record of Authorisations kept and maintained by him; input the data from the RIPA Request Form into the said register; complete the RIPA URN Request Form and email it back to the applicant and AO named on the form.

11 Role of Authorising Officer/s [AO] and Chief Executive (CEO)

11.1 A designated person called the "Authorising Officer" has the power to grant authorisations to carry out Directed Surveillance or CHIS. An applicant should always obtain authorisation from one before seeking judicial approval from the court. Those currently able to act as Authorising Officers for the Council are named in Appendix 2.

11.2 Note the on-going duties of Authorising Officers are described by IPC thus:

> "Responsibility for authorising an activity always remains with the Authorising Officer" – even after judicial approval. This includes reviewing and renewing authorisations as appropriate, and cancelling them promptly once the operation has been completed, rather than waiting for the whole remaining time to run out.

11.3 AOs are urged not to "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." There is a big difference between the type of operations conducted by the police and those run by Trading Standards.

11.4 It is the statutory responsibility of the Authorising Officer to establish that proposed action is both necessary and proportionate, whereas the role of the applicant is to present the facts, giving details of the crime, proposed activity, and justification for acting covertly etc. The case for the warrant should be presented in a fair and balanced way. All reasonable efforts should be made to take account of information which support or weakens the case for authorisation.

11.5 Authorising Officers should set out in their own words that s/he is satisfied or believes how and why the activity is necessary and proportionate. AOs should routinely state "who, what, when, where, how" i.e. who is to be the target of the surveillance; what action is being authorised; when it is to take place; where or at which location; and how the activity is to be done. Care must be taken over the use of words that could unintentionally limit the action – for instance using 'and/or' to permit both alternatives may be necessary to avoid unintended limitation - as wording in authorisations permitted by the court will be strictly construed.

11.6 A copy of the Authorisation Form is to be handed to the magistrate who considers the application. The AO will retain the original for safekeeping in the Council's RIPA records.

11.7 Authorising officers must conduct reviews of the activity as deemed necessary. The timing of such reviews must not be standardised or delayed, but as individual circumstances dictate and as seems prudent given the participants. Records of these reviews and issues considered must be recorded and available for inspection by the SRO and IPC.

11.8 The CEO is one of the Council's Authorising Officers, and, as Head of Paid Service, is the only one competent to approve any action or operation that involves the recruitment of a juvenile CHIS, or any other vulnerable person, or where the

surveillance may result in the Council obtaining access to legally privileged or confidential information.

12 The two Mandatory Tests for Directed Surveillance & CHIS

Necessity

12.1 An AO shall not grant an authorisation for the carrying out of Directed Surveillance and/or CHIS for a local authority unless s/he believes that the authorisation is necessary for the Prevention or Detection of Crime. In the case of Directed Surveillance, it must also meet the crime thresholds set out in para 4.4 above. The AO must carefully explain in writing why it's necessary to use the covert techniques requested.

Proportionality

12.2 An AO shall not grant an authorisation for the carrying out of directed surveillance and/or CHIS unless s/he also believes that the authorisation is proportionate to what is sought to be achieved [RIPA 2000, Ss 28(2)(b) & 29(3)].

13 Proportionality – striking the balance

13.1 This involves thinking about how far it is necessary to go to achieve an objective. The AO must show s/he has balanced a number of factors:

- The seriousness of the intrusion into the private or family life of the target - and any other person likely to be affected (collateral intrusion);

AGAINST:

- 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.

13.2 In simple terms – officers CANNOT use a 'sledge hammer to crack a nut'.

13.3 But they should also explain why the particular covert method, technique and tactic is the least intrusive, and why any alternatives considered would not be adequate (See Note 73 of the IPC 2016 Procedures & Guidance). The authorising officer must take into account the risk of obtaining private information about persons who are not the subjects of the surveillance or property interference activity. 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. An application should include an assessment of the risk of collateral intrusion and any details of any measures taken to limit this.

13.4 In brief, the AO needs to clearly articulate exactly 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 subjects of the surveillance activity (collateral intrusion). The AO's considerations need to be fully documented.

14 Judicial Approval

14.1 An Authorisation (or Renewal) for Directed Surveillance, or a CHIS does not become activated until judicial approval has been obtained in writing from a Magistrate/District Judge and is both dated and timed.

14.2 In order to apply for Judicial Approval, the applicant must do the following:-

a) Email the Single Point of Contact [SPOC] at Redbridge Magistrates Court [RMC]

b) SPOCs remain [Brian Gilbert)

c) The email must request a listing for an Application for Judicial Approval for a RIPA Application/Renewal.

d) Please ensure that sufficient notice is given to the court to list the matter prior to the date you wish to commence the operation

e) Complete Form Annex B, page 1

f) Please note all the information set out in the "Summary of Details," should also be contained in the Application/Renewal/Authorisation Form too, or the Application will NOT be granted

g) Please note that the applicant cannot solely rely on the details provided during his Evidence to the Court. Instead all relevant information must be set out in writing in the Application and Form B

h) Attend RMC for the Applications Court at the allotted time [i.e. 9.30am or 1.30pm]

i) Officers must take the Original Application/Renewal/Authorisation and copies along with 2 copies of the Judicial Approval Form Annex B

j) Provide a set of papers to the Court Clerk at least 30 minutes before the hearing, so the Magistrate can consider the paperwork prior to the hearing

k) When the hearing commences, the Applicant must swear on oath OR affirm

l) The Applicant is to identify him/herself by name, post and employer

m) The Applicant should introduce it as an Application for Judicial Approval for RIPA Authorisation or Renewal

n) The Applicant should introduce him/herself as the officer who has completed the paperwork for LBR's AO and the Court

o) S/he should Identify that the Application/Renewal etc was granted by LBR's AO [give name] on date and time and state the role/position of the AO

p) The Applicant should state that s/he wishes to obtain Judicial Approval for Directed Surveillance or use of a CHIS [Section 38 POFA].

q) The Applicant should inform the Magistrate that s/he has partly completed Form Annex B page 1.

14.3 Factors to be considered by the Magistrate

1) The Magistrate MUST be satisfied that:-

2) There were reasonable grounds for the local authority to believe that the Authorisation/Renewal etc was necessary and proportionate;

3) There remain reasonable grounds for believing that these requirements are still satisfied at the time of the application to the Magistrate;

4) Has the Application/Renewal etc been authorised by an appropriate Authorising Officer?

5) Has the Authorisation etc been made in accordance with any applicable legal restrictions e.g. has the Crime Threshold Test clearly been met?

6) In the case of a CHIS, were there reasonable grounds for believing that the arrangements exist for the safety and welfare of the source, AND that there remain reasonable grounds for believing that these requirements are satisfied at the time when the Magistrate/District Judge is considering the matter.

14.4 Outcomes

There are 3 possible outcomes for an Application for Judicial Approval:-

1) Box 1 --> Application Granted --> effective from that date and time

2) Box 2 --> Refuse to grant or renew the Authorisation [Applicant can then re-apply once the gap/error has been corrected]

3) Box 3 --> Refuse to grant or renew the Authorisation AND quash the AOs Authorisation

[Please note the Magistrate/District Judge 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]

14.5 Procedure once Judicial Approval Granted

1) If granted, the Authorisation/Renewal will be dated and timed, and the 3 months (for DS) or 12 months (for a CHIS) validity will run from this date and time.

2) The Magistrates will keep a copy of the completed and signed Form Annex B

3) The Applicant will be provided with the Original signed version of Form Annex B.

4) If the Application is for Directed Surveillance or CHIS, please provide the Principal Solicitor & Deputy Head of Litigation with the Original Judicial Approval Form Annex B within 14 days, and retain a scanned copy in your electronic investigation

file as a record and in order to fulfil Disclosure obligations if the matter proceeds to a criminal prosecution.

5) Applicants and AOs should be proactive about diarising, renewing and cancelling authorisations as appropriate.

15 Forms to be used

15.1 The following link should be used at all times, to access the Home Office's website RIPA Form page:-

https://www.gov.uk/government/collections/ripa-forms--2

15.2 Separate Directed Surveillance and CHIS forms can be found here, as can forms required for the renewal and cancellation of both types of activity.

15.3 Care should be taken with these forms, as they have not been revised since 2007 and cover the circumstances for a wide variety of other bodies, including the Police and Security Services.

16 Record Keeping

16.1 Records should be maintained centrally in accordance with Section 8 of the Code of Practice.

16.2 Records must be available for inspection by the Investigatory Powers Tribunal ('IPT'), established under Part IV of the 2000 Act, to carry out its functions (see chapter 11 of the Code of Practice for more information on the IPT). 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 (see section 67(5) of the Act), 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.

17 Data Protection Act 2018

17.1 Care must be taken to ensure that information received through directed surveillance is handled in accordance with the relevant legislative requirements and in accordance with the Council's information governance requirements.

17.2 Dissemination, copying and retention of material must be limited to the minimum necessary for authorised purposes.

17.3 Destruction

Information obtained through covert surveillance or property, interference, and all copies, extracts and summaries which contain such material, should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer needed for the authorised purpose(s) as set out in paragraph 9.5 of the Code. If such information is retained, it should be reviewed at appropriate intervals to confirm that the justification for its retention is still valid. In this context, destroying material means taking such steps as might be necessary to make access to the date impossible.

18 Other Useful Definitions & Guidance

18.1 Confidential Information

Confidential 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 privilege [solicitor and client] requires particular consideration – see paragraphs 9.23-9.72 of the Code. Unwarranted access to them during an investigation may be grounds for cancelling the Authorisation.

18.2 Duration of Authorisation

3 months for DS or 12 months for a CHIS from grant of Judicial Approval, but 4 months for a juvenile CHIS.

18.3 Reviews

18.3.1 Regular reviews are required once the authorisation has been granted, the frequency should be determined by the AO at the outset. If it is intended to be a short operation, a timely review should be conducted shortly thereafter, to determine if the authorisation is still required or if the operation is complete, which would then require the operation to be cancelled [see below].

18.3.2 Any proposed or unforeseen changes to the nature or extent of the activity that may result in the further or greater intrusion into the private life of any person should also be brought to the attention of the authorising officer by means of a review. The authorising officer should consider whether the proposed changes are proportionate before approving or rejecting them. Any such changes must be highlighted at the next renewal, if any. Where unidentified individuals become identified the terms of the authorisation should be refined at a review to include the identity of these individuals. It would be appropriate to convene such a review specifically for this purpose. This process will not require a fresh authorisation, providing the scope of the original authorisation envisaged surveillance of such individuals. Such changes must be highlighted at the next renewal if appropriate. During a review the reviewing officer may cancel aspects of the authorisation.

18.4 Renewals

18.4.1 Renewals must take place prior to the authorisation expiring; otherwise, the authorisation will automatically expire after 3 months. Please note, Judicial Approval is required for a Renewal and the Applicant must follow the procedure set out above. Please factor in sufficient time to obtain it well before the Authorisation expires.

18.5 Cancellation

18.5.1 The officer has a duty to request the AO to cancel the authorisation, where the authorisation no longer meets the criteria upon which it was originally authorised i.e. the test purchases are undertaken within 14 days, thereafter the authorisation is no longer required. In such cases, it is not permissible (nor

good practice) to let the authorisation run on until its natural expiry. Officers must be pro-active in this.

18.5.2 Good practice is for a record to be kept of the product which was achieved from the Surveillance.

19. Central Retrievable Record of Authorisations

19.1 A centrally retrievable record ("CRR") of all authorisations is held by the Council and regularly updated whenever an authorisation is granted, renewed or cancelled. The record should be made available to the relevant Commissioner or an Inspector from the IPC upon request. These records should be retained for a period of at least 7 years from the ending of the authorisations.

19.2 LBR's CRR of all authorisations is kept and maintained by the Operational Director of Assurance. Please see paragraph 10 regarding the mandatory requirement to complete a RIPA Request Form to obtain an URN from the Principal Solicitor and Deputy Head of Litigation.

19.3 All original applications, reviews, renewals and cancellation forms are to be served by hand, on the Operational Director of Assurance within 14 days of grant of Judicial Approval, to be stored in locked cabinets. On receipt, the relevant information is inputted, so as to update the CRR of Authorisations.

19.4 To avoid any suggestion that an authorisation 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 machine-prepared one. The Council must be ready to provide the relevant witness if authenticity is ever questioned in Court.

19.5 As recommended by the IPC, the Council will maintain a separate auditable record of any decisions and actions out with RIPA available to the SRO for scrutiny.

20. Senior Responsible Officer

20.1 Under the relevant Regulations the SRO is responsible for:-

- the integrity of the process in place within the public authority for the management of CHIS;
- compliance with Part II of the Act and with the relevant Code Of Practice
- prompt reporting of errors in accordance with the revised Code of Practice to the IPC and the identification of both the cause(s) of errors, and the implementation of the processes to minimise repetition of errors;
- responsible for ensuring that all AOs are of an appropriate standard addressing any recommendations and concerns in the inspection reports prepared by the IPC;
- engagement with the IPC inspectors when they conduct their inspections, where applicable; and
- where necessary, oversight of the implementation of post inspection action plans approved by the IPC.

20.2 Within a Local Authority, the SRO must be a member of the corporate leadership team. To avoid role conflict, the SRO should never act as an AO.

20.3 Please see Appendix 1 for the current SRO details.

21. RIPA for Redbridge CCTV

21.1 Directed Surveillance requests for access to Redbridge CCTV must be authorised by either Assistant Commissioner (Confidential Material Only) or Superintendent.

21.2 Requests are to be authorised by the Head of Service and a copy of the authorisation to be held on secure file by the CCTV manager.

21.3 The CCTV manager will issue the instruction of the CCTV Team with unique reference regarding authorisations for authorised directed surveillance.

21.4 Records are to be retained for inspection by the IPCO.

22. RIPA Reviews/Reports

22.1 Given the substantial reduction in the use of RIPA powers since 2013, LBR only hold meetings to review the operation of RIPA as and when deemed necessary by the SRO, or if requested by the AOs or any Head of Department using RIPA. Reports are made to the Corporate Management Team as necessary.

22.2 It is intended that members will receive a report at least annually to allow them to consider and review the adequacy of the Council's policy and practice on RIPA matters. The Council's policy and procedures are reported to Cabinet for formal approval, and the Governance & Assurance Committee will oversee the Council's use of RIPA by carrying out a high level annual review.

23. Social Media

23.1 The Council recognises that whilst many social media sites are freely accessible, just because officers can view them openly as part of their investigations, it does not mean that they should do so without regard to the constraints of the RIPA legislation.

23.2 Simple reconnaissance of social media and other sites are unlikely to interfere with a person's reasonable expectation of privacy and is unlikely to interfere with a person's reasonably held expectation of privacy.

23.3 Repetitive viewing of social media sites with any individual's personal details, interests and friendship networks for some covert purpose of which the target is unaware may amount to directed surveillance if it is done for the purpose of gathering intelligence or data to further an investigation into potential criminal activity.

23.4 The nature of the online platform may result in a reduced expectation of privacy where information is shared and openly available within the public domain. However, privacy implications may still apply regardless of whether or not the individual has made use of privacy settings.

23.5 The same considerations of privacy arise, and especially issues of collateral intrusion against innocent third parties, regardless of technological advances.

23.6 The creation of fake profiles and befriending of individuals must also be considered as potential manipulation of the 'relationship' created. This could also amount to the deployment of a CHIS, which requires prior authorisation by the Court to make it lawful. An example would be where officers create fake profiles to investigate someone suspected of selling counterfeit goods.

23.7 Any officer wishing to deploy such tactics as part of an investigation must remember before seeking a URN from Principal Solicitor & Deputy Head of Litigation and seeking judicial approval, that without appropriate authorisation, any evidence collected may be deemed inadmissible in any subsequent prosecution. Cases should be carefully considered on an individual basis, and the issues of necessity and proportionality always borne in mind. Note 289 of the IPC Procedures and Guidance contains more suggestions.

23.8 The foregoing paragraphs under this section should be read in conjunction with the guidance contained in the updated Codes of Practice (links attached) which offers some helpful examples:

- For Surveillance – see paragraphs 3.10 to 3.17 -

  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

- For CHIS – see paragraphs 4.11 to 4.17 -

  https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

24. Aerial Covert Surveillance

24.1 Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (colloquially known as 'drones'), is planned, consideration should be given as to whether a surveillance authorisation is appropriate.

25. Training & Monitoring

25.1 In order to be an AO, all officers must have attended a suitable training course. Any new AO will be appointed by the SRO, who will ensure that all AO's receive regular updates and training, as and when required. All officers utilising RIPA for Directed Surveillance and/or CHIS must also have attended suitable training course.

25.2 Whilst undertaking audits of the RIPA CRR of Authorisations and RIPA forms, the SRO will identify any training needs for staff and/or monitoring issues, to be raised either with individual AO's and/or at any RIPA Meetings.

25.3 The Council's policy commitment is that RIPA training will be provided to staff on a regular rather than ad hoc basis. However, where staff already receive training as part of their professional accreditation, (e.g. ACFS or ACFP) that can be taken into account when assessing their needs.

26. Investigatory Powers Commissioner

26.1 The IPC (formerly the OSC) is the supervisory body for RIPA and deals with the following in particular:-

- Requests for RIPA Statistical Information twice per year [March & December]
- Inspections of Local Authorities including LBR usually every 2 to 3 years
- Publication of regular reports on RIPA activity

26.2 The IPC also publishes a Procedures and Guidance booklet on the use of RIPA by public authorities, most recently in 2016 (IPC 2016). It can be found at:

https://IPC.independent.gov.uk/wp-content/uploads/2016/07/IPC-Procedures-Guidance-July-2016.pdf

It has no binding legal authority, and merely expresses the opinions of the IPC. But inspections will be conducted in accordance with its recommendations, and it recommends that all AOs should have a personal copy for reference.

27. Collaboration with other authorities/agents

27.1 The Council will endeavor to conclude written collaboration agreements with any other authorities with whom it works regularly, such as the Police or neighbouring Trading Standards Authorities as recommended by OSC 2016.

27.2 Prior to any activity, where the Council uses external partners or agents, as advised in OSC 2016 para 112, the Council will seek their written acknowledgement that they

- Will act as an agent of the Council, and
- Have seen the written Authorisation for the activity they are undertaking, and
- Will comply with the specific requirements permitted by the Authorisation, and
- Recognise they may be subject to inspection by the IPC for RIPA activity.

28. Codes of Practice

28.1 The Home Office publishes Codes of Practice giving guidance on the use of RIPA by public authorities. The current editions were published in 2018 pursuant to section 71 of RIPA 2000. There is a separate Code concerning Communications Data which is not covered in this Manual.

28.2 Unlike the IPC guidance, the **Home Office Codes are admissible in evidence** in any court proceedings, and **must be taken into account**. Public authorities like the Council may be required to justify the use, granting or refusal of authorisations by reference to the Codes.

28.3 Care must be taken when referring to the Codes over the terminology used, and to their applicability to the Council. The Codes provide guidance to a much wider range of public authorities than the Council. Unfamiliar terms like “relevant sources” may not apply to the Council at all, and may confuse the lay reader. Please ensure you seek legal advice on correct interpretation before applying advice you may find there.

28.4 The two Codes now in force and of concern to the Council are accessible through the Home Office website:

Covert Surveillance & Property Interference Code of Practice
Covert Human Intelligence Sources

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

The Investigatory Powers Tribunal has jurisdiction to investigate and determine complaints against public authority use of investigatory powers

APPENDICES

APPENDIX 1	Current SRO and contact details
APPENDIX 2	Authorising Officers, names and contact details
APPENDIX 3	Prosecution Lawyer, name and contact details
APPENDIX 4	Communications Data Designated Person & contact details
APPENDIX 5	Trading Standards' Work Instruction 2013 (NAFN & Judicial Approval)
APPENDIX 6	RIPA URN Request Form
APPENDIX 7	Annex B – Judicial Approval Form
APPENDIX 8	Home Office Directed Surveillance Authorisation Form
APPENDIX 9	Home Office CHIS Authorisation Form
APPENDIX 10	RIPA Decision Chart

Appendix 1

The Senior Responsible Officer at the date of publication of this Manual is:

Operational Director of Assurance

Appendix 2

The Authorising Officers are:

Claire Symonds, Chief Executive, Head of Paid Service; Tel: 020 8708 2100
Sasha Taylor, Head of Community Protection and Licensing: Tel: 020 8708 4792.
Emma Vick, Counter Fraud Manager: Tel: 020 8708 5255
Pervinder Sandhu – Operational Director Assurance and general queries: Tel: 020 8708 2168

Appendix 3

Prosecutions Lawyer: Tel: 020 8708 2865

Appendix 4

The Communications Data Designated Person is Sasha Taylor, Head of Community Protection and Licensing: Tel: 020 8708 4792.

Items 5 – 10 are attached.