BRENT COUNCIL'S RIPA POLICY AND PROCEDURES

July 2017

BRENT COUNCIL'S RIPA POLICY AND PROCEDURES

Contents

APPENDICES

1. Introduction

1.1 This document explains the Council's use and conduct of covert surveillance techniques when investigating serious criminal offences relying on the powers made available to local authorities in Part II of the Regulation of Investigatory Powers Act 2000 (RIPA). RIPA makes surveillance authorised in accordance with the statutory framework it establishes lawful and thereby protects the Council from legal claims and complaints and ensures that the evidence it relies upon in prosecutions is admissible.

1.2 Covert surveillance techniques include static surveillance (e.g. taking up an observer post to monitor the activities and movements of those suspected of having committed criminal offences); mobile surveillance (e.g. following someone to see where they are going without their knowledge); using hidden CCTV at a crime hotspot and the use of undercover officers and informants.

1.3 This document also contains some information about accessing communications data such as out-going phone calls and websites visited held by telephone and internet service providers. However, only limited information about who sent the communication, when and how can be accessed but not the content i.e. what was said and written. This form of surveillance is regulated by a different part of RIPA and different procedures apply i.e. authorisations are granted by a national body which acts on behalf of local authorities.

1.4 As well as the current legislation, the Council's policies and procedures are informed by statutory codes of practice issued by the Home Office in December 2014. Namely, the Covert Surveillance etc. Code of Practice and Covert Human Intelligence Sources Code of Practice.

1.5 The Council's use and conduct of covert surveillance techniques is overseen internally by the Council's Monitoring Officer, who also acts as the Council's Senior Responsible Officer (SRO) for the purposes of the Home Office Codes of Practice, and externally by the Office of Surveillance Commissioners (OSC). The OSC conduct periodic inspections of public authorities entitled to exercise RIPA powers in order to fulfil their oversight role. The OSC also issue technical Guidance to public authorities and this document is informed by its current Guidance issued in July 2016.

1.6 The Council's policies and procedures have been approved by Cabinet. In addition, the Audit Advisory Committee will carry out a high level annual review of any authorisations granted or renewed, initially by an Authorising Officer of the Council and subsequently by a magistrate, in accordance with the requirements of RIPA.

1.7 Compliance with the policies and procedures agreed in this document is mandatory for all relevant Council services and officers. RIPA powers are now predominantly used to enforce trading standards controls and, in particular, to conduct test purchases of age restricted products such as alcohol. It is also occasionally used in the context of serious fraud investigations. It remains essential, however, that all potential users are fully aware of the contents of this document.

2. Definition of Surveillance

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.

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 numbers [Section 26 (10)], which are also covered by the Data Protection Act 1998.

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.

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 either a person on the premises/in the vehicle or a surveillance device even if it is not on the premises or in the vehicle if it provides information of the same quality as if it was. Surveillance of premises used for the purpose of legal consultations is also regarded as Intrusive Surveillance.

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 <u>target</u> must be <u>unaware</u> that it is or could be taking place;
- it must be done in a way likely to obtain <u>private information</u> about the target;
- it must <u>not</u> be an <u>immediate response</u> 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 <u>**not**</u> apply to the use of a <u>**CHIS**</u>.

5. <u>Basis for Lawful Surveillance Activity</u>

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 <u>provided</u> 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 minimum crime threshold.

5.6 From 1st October 2015 the 2010 Regulations were amended further - to add that the potential offence/s may relate to the purchase of alcohol <u>on behalf</u> of those under 18 (proxy purchases), or the sale of <u>nicotine products</u> 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 policy and procedures on non-RIPA surveillance, and keep appropriate written logs of activity open to scrutiny by the SRO as recommended in Note 80 in OSC 2016 Guidance and Procedures.

6. <u>Directed Surveillance Example</u>

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. <u>Communications Data</u>

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 Deputy Chief Legal Officer and his contact details also appear in Appendix 4.

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.

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);
(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 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

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

9. Becoming a CHIS and ‘status drift’

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 LBB 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 may become one. This situation is referred to by the OSC 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 OSC 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.

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.

10. Requirement to obtain a URN from Legal Services

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 Prosecution Lawyer, 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 Prosecution Lawyer 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 Officers [AOs] and the special role of the Chief Executive

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 OSC 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.

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 OSC.

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 officer 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:

- the gravity and extent of the perceived mischief;
- the size and scope of the surveillance;
- the need for the activity in operational terms;
- the benefit expected from it;
- alternative (possibly less intrusive) methods of getting the information;
- how to mitigate any intrusion.

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

13.3 Officers must explain why the particular covert method, technique and tactic is an appropriate use of RIPA and a reasonable way of achieving the desired objective. In particular, officers must explain why the intended surveillance will cause the least possible intrusion, and what alternative options have been tried or considered and why they were unsuccessful or not considered suitable (See Note 73 of the OSC 2016 Procedures & Guidance).

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 Willesden Magistrates Court [WMC]

b) **SPOC**s remain Philip Cunningham [philip.cunningham@hmcts.gsi.gov.uk] or Andrew Wood [andrew.wood1@hmcts.gsi.gov.uk]

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 WMC 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 LBB and the Court

o) S/he should Identify that the Application/Renewal etc was granted by LBB'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 <u>Factors to be considered by the Magistrate</u>

The Magistrate MUST be satisfied that:-

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

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

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

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

v) 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

14.5.1 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.

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

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

14.5.4 If the Application is for Directed Surveillance or CHIS, please provide the Prosecution Lawyer 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.

.14.5.5 Please note that the Authorisation will automatically expire unless a Renewal Application is made prior to its expiration and Judicial Approval is also obtained.

14.5.6 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. Other useful definitions and guidance

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]. Unwarranted access to them during an investigation may be grounds for cancelling the Authorisation.

Duration of Authorisation

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

Reviews

Regular reviews are required once the authorisation has been granted, the frequency should be determined by the AO. 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].

Renewals

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.

Cancellation

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.

17. Central Record of Authorisations

17.1 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 OSC upon request. These records should be retained for a period of at least 7 years from the ending of the authorisations.

17.2 LBB's CRR of all authorisations is kept and maintained by the Principal Prosecution Lawyer. Please see paragraph 10 regarding the mandatory requirement to complete a RIPA Request Form to obtain an URN from him.

17.3 All original applications, reviews, renewals and cancellation forms are to be served by hand, on the Principal Prosecution Lawyer 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.

17.4 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.

17.5 As recommended by the OSC, the Council will maintain a separate auditable record of any decisions and actions outwith RIPA available to the SRO for scrutiny.

18. Senior Responsible Officer (SRO)

18.1 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 to the OSC and the identification of both the cause(s) of errors, and the implementation of the processes to minimise repetition of errors;
- engagement with the OSC inspectors when they conduct their inspections, where applicable; and
- where necessary, oversight of the implementation of post inspection action plans approved by the OSC.

18.2 Within a Local Authority, the SRO must be a member of the corporate leadership team, and is responsible for ensuring that all AOs are of an appropriate standard in light of any recommendations in the inspection reports prepared by the OSC. To avoid role conflict, the SRO should never act as an AO.

18.3 Please see Appendix 1 for the current SRO details.

19. RIPA Reviews/Reports

19.1 Given the substantial reduction in the use of RIPA powers since 2013, LBB 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.

19.2 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 Audit Advisory Committee will oversee the Council's use of RIPA by carrying out a high level annual review.

20. The use of the internet and social media for investigative purposes

20.1 With advances in technology making it easier, quicker and increasingly popular for individuals to share personal information on-line, the opportunities to use that information for research, investigative or other official purposes are expanding too.

20.2 However, it is important to appreciate that the considerations of privacy which arise in the physical world also arise in the on-line world. In other words, there are rules and there are limits.

20.3 Just because the content of many social media sites and other information on the internet is freely accessible does not mean that officers can openly access such information without careful regard to the constraints and requirements of the law.

20.4 Repeated or systematic viewing, collecting or recording of private information from 'open' on-line sources (such as Facebook, Twitter, Snapchat and LinkedIn), including information relating to the interests, activities and movements of individuals, and others associated with them, could be regarded as a form of covert surveillance.

20.5 In addition, it is likely that individuals will have a reasonable expectation that their information is not used for surveillance purposes by public authorities and therefore may complain that their privacy and human rights have been infringed.

20.6 Initial research of social media to establish or check some basic facts is unlikely to require an authorization for directed surveillance, <u>but repeated visits to build a profile of an individual's lifestyle etc. is likely to do so depending on the particular facts and circumstances</u>. This is the case even if the information is publicly accessible because the individual has not applied any privacy settings.

20.7 The creation of fake profiles or any attempt to make 'friends' on-line for the covert purpose of obtaining information may constitute directed surveillance or, depending on the nature of the interaction or the manipulation of the relationship, a CHIS. An example would be where officers create fake profiles to investigate someone suspected of selling counterfeit goods.

20.8 Any officer wishing to deploy such tactics as part of an investigation must remember before seeking internal authorization and judicial approval, 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 OSC Procedures and Guidance contains more practical guidance.

20.9 It is also important to appreciate that if officers obtain, use or even merely store information about individuals they will have to comply with data protection rules. And, when the General Data Protection Regulation comes into force on 25 May 2018, the information the Council collects about individuals, how and why will have to comply with stricter transparency and accountability rules.

21. <u>Training & Monitoring</u>

21.1 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 a suitable training course.

21.2 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.

21.3 The Council's policy commitment is that RIPA training will be provided to staff every three years. 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.

22. <u>Office of Surveillance Commissioners (OSC)</u>

22.1 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 LBB usually every 2 to 3 years
- Publication of regular reports on RIPA activity

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

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

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

<u>23. Collaboration with other authorities/agencies</u>

23.1 The Council will endeavour 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.

23.2 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 OSC for RIPA activity.

24. <u>Codes of Practice</u>

24.1 The Home Office publishes Codes of Practice giving guidance on the use of RIPA by public authorities. The current editions were published in 2016 pursuant to section 71 of RIPA 2000. There is a separate Code concerning Communications Data which is not covered in this Policy.

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

24.3 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.

24.4 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

APPENDICES

APPENDIX 1: Senior Responsible Officer (SRO) Contact Details

Debra Norman, Interim Chief Legal Officer and Monitoring Officer: Debra.Norman@brent.gov.uk; 020 8937 1578

APPENDIX 2: List of Authorising Officers and Contact Details

Carolyn Downs, Chief Executive/Head of Paid Service: Carolyn.Downs@brent.gov.uk; 020 8937 1101

Conrad Hall, Chief Finance Officer: Conrad.Hall@brent.gov.uk; 020 8937 6528

Chris Whyte, Operational Director Environment Services: Chris.Whyte@brent.gov.uk; 020 8937 5342

Simon Legg, Head of Trading Standards: Simon.Legg@brent.gov.uk; 020 8937 5522

APPENDIX 3: Prosecution Lawyers

Tola Robson, Senior Advocate: Omotolani Robson: Omotolani.Robson@brent.gov.uk; 020 8937 1455)

Priscilla Pryce, Senior Legal Assistant: Priscilla.Pryce@bent.gov.uk; 020 8937 4330

APPENDIX 4: Communications Data Senior Responsible Officer (SRO) and Designated Person Contact Details

Communications Data Senior Responsible Officer (SRO): Arnold Meagher, Deputy Chief Legal Officer: Arnold.Meagher@brent.gov.uk; 020 8937 2166

Communications Data Designated Person: Simon Legg, Head of Trading Standards: Simon.Legg@brent.gov.uk; 020 8937 5522

The following appendices are attached to this document:

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