Appendix A: Key changes which have been inserted into the RIPA policy and procedures.

The following sections highlighted in red have been inserted into the RIPA policy and procedure. The numbering reflects the current numbering in the policy.

6.3 Aerial Covert Surveillance

6.3.1 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 an aerial surveillance authorisation is appropriate.

……

7. Communications Data

7.1 As part of an investigation, there are occasions when "Communications Data" (CD) is permitted to be obtained from a Communications Service Providers ("CSPs").

7.2 Communications Data includes the 'who', 'when', 'where', and 'how' of a communication, but Local Authorities are prohibited from obtaining the content of any communication i.e. what was said or written. It is generated, held or obtained in the provision, delivery and maintenance of communications services i.e. postal services or telecommunications services.

All communications data held by a telecommunications operator or obtainable from a telecommunication system falls into two categories of entity data and events data; and Local Authorities may only acquire less intrusive types of Communications Data:

(i) "Entity data" (e.g. subscriber information such as the identity of the person to whom services are provided, address and customer information); includes:

- 'subscriber checks' such as "who is the subscriber of phone number 01234 567 890?", "who is the account holder of e-mail account example@example.co.uk?" or "who is entitled to post to web space www.example.co.uk?";
- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services; or

(ii) "Events data" (e.g. the date and time sent, duration, frequency of communications, call diversion and IP address information) includes, but is not limited to:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);

- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);

- itemised telephone call records (numbers called);

- itemised timing and duration of service usage (calls and/or connections);

7.3 Part 3 of the Investigatory Powers Act 2016 (IPA) contains the provisions that now govern the powers available to the Local Authorities for the lawful acquisition of CD. Some of the key parts of Part 3 came into force on 11 June 2019 and replace many of the provisions relating to acquisition of CD under RIPA.

7.4 Under the IPA and for the purpose of acquiring CD, the role of the Designated Person (DP) within the Local Authority (LA) and the Magistrate/District Judge is abolished. The authorising role of the DP and the Magistrate / District Judge is now replaced by a new independent body called the Office for Communications Data Authorisations (OCDA).

7.5 Further the Data Retention and Acquisition Regulations 2018 (SI 2018/1123) ("DRAR") amend Parts 3 and 4 of the IPA which provides for the retention of Communications data by telecommunications and postal operators, and the acquisition of that communications data by public authorities.

7.6 The DRAR introduced the new code of practice entitled "Communications Data Code of Practice" about the exercise of functions conferred by Parts 3 and 4 of the IPA (Regulation 2).

7.7 As a matter of policy and practice, the Council's Communications data activities have been outsourced to the National Anti-Fraud Network ("NAFN"). The IPA has now codified this process. Local Authorities **must now** submit all their Communications data applications, via, NAFN, for the consideration of the OCDA. This effectively means that NAFN will continue to be the Single Point of Contact ("SPoC) for all applications made by Brent Council.

7.8 However before submission to NAFN, the application must be brought to the attention of the Designated Senior Officer who has been given the designated role of overseeing the applications before submission to NAFN. The details of the Designated Senior Officer appears in Appendix 4.

7.9 Brent Council's Trading Standards Service collaborates and liaises with NAFN to ensure the provisions of the IPA are complied with and to ensure any application follows best practice.

7.10 For applications made for the acquisition of CD under the IPA, the "applicable crime purpose" must be met concerning all applications for both *Entity Data* and *Events Data.*

7.11 The applicable crime purpose is defined differently depending on the data type. Where the Communications Data sought is *Entity Data*, the applicable crime purpose is the prevention or detection of crime or the prevention of disorder.

7.12 In cases where the Communications Data required is wholly or partly *Events Data*, the applicable crime purpose is defined as preventing or detecting serious crime (the "serious crime threshold"). The *serious crime threshold* under IPA includes offences where an adult may be sentenced to at least 12 months or more in prison (and any offence committed by a body corporate).

……..

8. Covert Human Intelligence Sources [CHIS]

8.2 The key difference between Directed Surveillance and use of 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. Any manipulation of a relationship amounts to a fundamental breach of trust, which depending on the covert purpose can place a CHIS in serious danger. Consequently, extra precautions may be required to ensure a CHIS is not discovered.

……..

9.8 The use and wearing of recording devices is done in accordance with the College of Policing Body Worn Video Guidance 2014. Following the case of AB v Hampshire Constabulary IPT/17.191/CH (5.2.19) it should be noted the video recording body worn camera is capable of amounting to surveillance within the meaning of Part 11 RIPA 2000.

…….

13. Proportionality – striking the balance

13.1 This involves considering a number of factors as highlighted by s4.7 of the Code:

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

……

16.1 RIPA for Brent Council CCTV

16.1.1 Directed Surveillance requests for access to Brent Council's CCTV must comply with the RIPA CCTV protocol.

16.1.2 The Council will only allow the Police and other third parties to use its CCTV systems to carry out targetted covert surveillance (which includes the disclosure of recordings) in the Borough of Brent if the requirements of the protocol are adhered to.

16.1.3 All visitors to the CCTV room must also complete the visitors' signing-in book giving relevant details of the operation involved and the specific CCTV camera(s) to be used.

16.1.4 Records are to be retained for inspection by the Information Commisioner's Office (IPC), Surveillance Camera Commissioner (SCC), IPCO and SRO as and when required.

……

18. Senior Responsible Officer (SRO)

18.1 Under the relevant Home Office Codes for surveillance, CHIS and Communications Data, the SRO is responsible for-

- the integrity of the process in place within the public authority for the management of CHIS and to acquire communications data.
- engagement with officers in the Office for Communications Data Authorisations (where relevant).
- compliance with Part II of the RIPA 2000 and Part 3 of IPA and with the relevant Codes Of Practice
- oversight and prompt reporting of errors in accordance with the Codes of Practice to the IPCO and the identification of both the cause(s) of errors, and the implementation of the processes to minimise repetition of errors; (an example of such an error would be carrying out surveillance without proper authorisation);
- ensuring the overall quality of applications submitted to OCDA by the Council.
- engagement with the IPCO inspectors when they conduct their inspections; and
- where necessary, oversight of the implementation of post inspection action plans approved by the IPCO.

……

Codes of Practice

24.1 As mentioned above 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 detail in this Policy.

24.2 Unlike the OSC and IPCO 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.

……

25 Data Protection Act 2018

25.1 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.

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

……

26. Consequences of non –compliance with RIPA

Where covert surveillance work is being proposed for matters which fall within the ambit of RIPA 2000, this Policy and procedure must be strictly adhered to in order to protect both the Council and individual officers from the following:

26.1 **Inadmissible Evidence and Loss of a Court Case:** there is a risk that, if Covert Surveillance and Covert Human Intelligence Sources are not handled properly, the evidence obtained may be held to be inadmissible in court proceedings by virtue of s78 Police and Criminal Evidence Act (PACE) 1984. Section 78 allows for evidence, that was gathered in a way that affects the fairness of the criminal proceedings, to be excluded. The Common Law Rule of Admissibility means that the court may exclude evidence because its prejudicial effect on the person facing the evidence outweighs any probative value the evidence has (probative v prejudicial test).

26.2. **Legal Challenge –**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.

26.3. **Censure** – the IPCO conduct regular audits on how Local Authorities implement RIPA and IPA. If it is found that a Local Authority is not implementing RIPA/IPA properly, then this could result in censure.

26.4 **Complaint to The Investigatory Powers Tribunal (**"IPT"**)**: 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. This Tribunal is made up of senior members of the judiciary and the legal profession. It is independent of the Government and has full powers to investigate and decide any case within its jurisdiction and award compensation. It 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.

26.5 Any action commenced in paras 26.1-26.4 above may have financial and reputational implications for the council as well as affect its ability to utilise RIPA.

27 Case to Note: Case of *Gary Davies v British Transport Police* (IPT/17/93/H)

27.1 On 30th April 2018, the IPT awarded £25k to reflect the gravity of the breach and damage suffered and a further award of £21,694 in respect of costs, totalling a compensation award of £46,694 to an individual who complained about surveillance by British Transport Police. This case involved surveillance carried out without proper authorisation and without proper compliance with all the relevant provisions of RIPA 2000. The tribunal indicated that in their view none of the officers involved in the matter demonstrated an adequate knowledge of the relevant requirements of RIPA. The Tribunal classified the unauthorised surveillance as "unlawful".

27.2 The above case shows that the importance and extent of financial penalties that can be imposed by failing to adhere to provisions of this Policy, the IPA, RIPA and the relevant Codes of Practice.