London Borough of Merton

Policy and Procedure

Regulation of Investigatory Powers 2000

MERTON COUNCIL'S RIPA POLICY AND PROCEDURES

Section Contents

APPENDICES

1. Introduction

1.1 This policy 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) and the Investigatory Powers Act (IPA) 2016.

1.2 RIPA authorises surveillance in accordance with the statutory framework making it lawful; and thereby protecting the Council from legal claims, complaints and ensuring that the evidence relied upon in prosecutions is admissible.

1.3 Covert surveillance techniques include:

a. static surveillance (for example, taking up an observer post to monitor the activities and movements of those suspected of having committed criminal offences);

b. mobile surveillance (for example, following someone to see where they are going without their knowledge);

c. using hidden CCTV at a crime hotspot and the use of undercover officers and informants; monitoring a person's activities on the internet or social media.

1.4 This policy 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 information about who sent the communication, for example, when and how can be accessed but not the content, that is, what was said and written.

1.5 As well as the current legislation, the Council's policies and procedures are informed by statutory Codes of Practice issued regularly by the Home Office, most recently in 2018 (namely, the Covert Surveillance etc. Revised Code of Practice and Covert Human Intelligence Sources Revised Code of Practice).

1.6 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 Investigatory Powers Commissioner's Office. The IPCO conducts periodic inspections of public authorities entitled to exercise RIPA powers in order to fulfil their oversight role.

1.7 The Council's policies and procedures have been approved by the Standards and General Purposes Committee which has an oversight role and carries out high-level annual reviews 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.

1.8 Compliance with the policies and procedures agreed in this document is mandatory for all relevant Council services and officers. RIPA powers are most

likely to be used to enforce trading standards controls and tackling fly-tipping and repeatedly fraudulent use of blue badges. It remains essential, however, that all potential users are fully aware of the contents of this document.

1.9 Where applicable and potentially helpful, relevant statutory provisions are referred to, 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.

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. It covers personal data like names, addresses and telephone numbers [Section 26 (10)], which are also covered by the Data Protection Act 2018 and the General Data Protection Regulation (GDPR).

3.3 Obtaining private information 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, recognising that there may be an expectation of privacy over information that 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. Intrusive surveillance is covert surveillance that:

a) covers anything taking place on/in any residential premises or a private vehicle,
b) involving either a person on the premises/or in the vehicle, or
c) is carried out by a surveillance device, (even if a device is not on the premises or in the vehicle if it provides information of the same quality and detail as if it was inside, this may amount to Intrusive Surveillance.

Surveillance of premises used for the purpose of legal consultations is also regarded as Intrusive Surveillance.

Directed Surveillance

4.3 Directed Surveillance must be:

a) for the purpose of a specific operation or investigation (relating to a statutory Enforcement function);

b) covert. Its target must be unaware that it is or could be taking place;

c) done in a way that is likely to obtain private information about the target;

d) planned. It must not be an immediate response to events.

4.4 Under the provisions of RIPA 2000, 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 term of at least 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 a Covert Human Intelligence Source (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. This is 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 which is 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. For example, the additional purposes of protection of public health, or in the interests of public safety, and the prevention of public disorder have all been removed.

5.5 To be sure a matter is RIPA controlled, officers must identify from the outset whether:

a) they are investigating a criminal offence - and if so,
b) whether it passes the minimum crime threshold.

5.6 From 1/10/2015 the 2010 Regulations were amended further - to add that the potential offences 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 offences are being investigated, or the penalties for them, legal advice should be taken from the Senior Enforcement 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 under RIPA will not be permitted.

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. Proportionality (discussed in paragraph 13 below), also applies 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. However, 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, 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 retains the right to exercise 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, where the crime threshold is not met, the Council will work in line with its policy and procedures on non-RIPA surveillance, and keep written logs of activity open to scrutiny by the SRO and IPCO. Further information appears in Appendix 6.

6. Directed Surveillance Example

6.1 An example of Directed Surveillance is a covert static post (for example, an officer in car outside an address with a camera) taking pictures of, and/or following a target who has claimed Direct Payment, on the basis that they are severely disabled to the extent that they cannot walk unaided nor drive. The Directed Surveillance is undertaken as it is alleged that the disabilities are invented and/or exaggerated by the target.

6.2 The surveillance scenario would be covert, as it is 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.

6.3 Aerial Covert Surveillance

Where surveillance using airborne crafts or devices, for example helicopters or unmanned aircraft (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 Provider ("CSP").

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, that is, what was said or written. CD includes the way in which, and by what method, a person or thing communicates with another thing or person. It excludes anything within a communication including text, audio and video that reveals the meaning of the communication. CD is generated, held or obtained in the provision, delivery and maintenance of communications services, that is, 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:

(a) "Entity data" (for example, subscriber information such as the identity of the person to whom services are provided, address and customer information); includes:

Page 17

- ‘subscriber checks’ such as “who is the subscriber of phone number 020 7224 3688”, “who is the account holder of e-mail account sherlock.holmes@Bakerstreet.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” (for example, 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 govern the powers available to the Local Authorities for the lawful acquisition of CD.

7.4 Judicial approval is a required before undertaking directed surveillance or use of a CHIS. The Office for Communications Data Authorisations (OCDA) makes independent decisions on whether to grant or refuse communications data requests, ensuring that all requests are lawful, necessary and proportionate.

7.5 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 must now submit all their Communications Data applications to NAFN (National Anti-Fraud Network), for the consideration of the OCDA. This means that NAFN will be the Single Point of Contact (“SPoC) for all applications made by Merton 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 The Regulatory Services Partnership (hosted by Merton Council provided the statutory regulatory functions for the three London Boroughs of Merton, Richmond upon Thames and Wandsworth) 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 In order for Merton to request CD under the IPA it must be necessary for the applicable crime purpose; and, 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
- any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;
- any offence committed by a body corporate;
- any offence which involves, as an integral part of it, the sending of a communication;
- any offence which involves, as an integral part of it, a breach of a person's privacy.

- An application for CD should also consider factors relating to proportionality as follows [3.16 of the Code]:

    - whether what is sought to be achieved could reasonably be achieved by other less intrusive means,
    - whether the level of protection to be applied in relation to obtaijning communications data is higher because of the particular sensitivity of that information, and
    - the public interest in the integrity and security of telecommunication systems and postal services.

7.13 A CD authorisation becomes valid on the date the authorisation is granted. It is then valid for a maximum of one month.

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

Page 19

7.15 Any staff considering the use of communications interception or other activity should contact the Designated Senior Officer to discuss the proposed action in order to obtain appropriate direction and guidance.

8. Covert Human Intelligence Sources [CHIS]

8.1 A CHIS is perhaps more commonly called an “informant”. A person is a CHIS if they:-

(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 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.

8.3 In order to grant an authorisation for using a CHIS, the Authorised Officer (“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)(iii)].

8.4 “Control” of a CHIS. Subsection (5) requires that arrangements are in place in respect of the CHIS for ensuring that:

(a) that there will be at all times a “handler” of the specified rank with the relevant investigating authority, with day to day responsibility for the source.

(b) that there will be at all times a “controller” of the specified rank with the relevant investigating authority with the general oversight of the use made of the source.

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

(d) that the records relating to the source that are maintained by the relevant investigating authority will always contain particulars of all such

matters (if any) as may be specified for the purposes of this paragraph in regulations made by the Secretary of State

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

"Relevant investigating authority," means the public authority for whose benefit the activities of that individual as such a source are to be undertaken. (**Note**: The Council may undertake 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, for example, 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 a case 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 they have covertly passed to Merton has been obtained in the course of (or as a consequence of he 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 known 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 RSP regularly undertake covert test purchasing, and task children to request a one-off sale. The Council 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 RSP operate policy and procedures based on guidance from the Trading Standards national body in such circumstances.

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.

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 Unique Reference Number from SLLP (Information Governance Team)

10.1 For Directed Surveillance that satisfies the Crime Threshold Test or for a CHIS, the officer must first obtain a Unique Reference Number [URN] for the operation from an Information Governance Officer, prior to the completion and/or submission of an application for Directed Surveillance and/or CHIS to an Authorising Officer (AO).

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

a) is DS/CHIS for the Prevention or Detection of Crime?

b) specify the criminal offence(s) being investigated and the statute(s)

c) for Directed Surveillance only, does the criminal offence(s) meet the Crime Threshold Test (at least the 6 months maximum sentence); **or**

d) is the offence(s) for underage sale/supply of alcohol or tobacco/nicotine?

e) (for DS and CHIS) is the action proposed both necessary and proportionate?

f) 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 Informaion Governance Officer will consider the contents; allocate an URN from the electronic Central Retrievable Record of Authorisations kept and maintained by them; 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 person appointed to the role of "Authorising Officer" has the power to grant authorisations to carry out Directed Surveillance or CHIS. An applicant must 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 IPCO as follows: "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 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 the 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 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 they are 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 or District Judge 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 kept and available for inspection by the SRO and IPCO.

11.8 The Chief Executive ("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, 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 must not grant an authorisation for the carrying out of Directed Surveillance and/or CHIS for a local authority unless they believe 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 paragraph 4.4 above. The AO must carefully explain in writing why it is 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 they 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 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.

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 paragraph 4.6 - 4.7 of the 2018 revised Codes).

13.4 The AO 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.

13.5 In brief, the AO must clear set out 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 the Assistant Head of Law, David Fellows (David.Fellows@merton.gov.uk)

b) the email must request a listing for an application for Judicial Approval for a RIPA Application/Renewal.

c) ensure that sufficient notice (5 days) so that the court can list the matter prior to the date you wish to commence the operation.

d) complete Form Annex B, 1st page (Appendix 5).

e) ensure 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.

f) 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.

g) attend WMC for the Applications Court at the allotted time [either 9.30am or 1.30pm].

h) take the Original Application/Renewal/Authorisation and copies along with 2 copies of the Judicial Approval Form Annex B.

i) provide a set of papers to the court legal adviser at least 30 minutes before the hearing, so the Magistrate/ District Judge can consider the paperwork prior to the hearing.

j) when the hearing commences, the Applicant:

- must swear an oath OR affirm;
- identify him/herself by name, post and employer;
- should introduce it as an Application for Judicial Approval for RIPA Authorisation or Renewal;
- should introduce themselves as the officer who has completed the paperwork for Merton LBC and the court;
- should identify that the Application/Renewal etc. was granted by Merton's AO [give name] on date and time and state the role/position of the AO
- should state that they wishes to obtain Judicial Approval for Directed Surveillance or use of a CHIS [Section 38 POFA];
- should inform the Magistrate/District Judge that they has partly completed Form Annex B page 1.

14.3 Factors to be considered by the Magistrate/ District Judge

The Magistrate /District Judge 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/ District Judge;

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, for example, 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:-

a) Application Granted - effective from that date and time;

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

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

[**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. The 3 months (for DS) or 12 months (for a CHIS) validity will run from this date and time. The Magistrates will keep a copy of the completed and signed Form Annex B. The Applicant will be provided with the Original signed version of Form Annex B.

14.5.2 If the Application is for Directed Surveillance or CHIS, the Information Governance Officer should be provided with the Original Judicial Approval Form Annex B within 5 days, and retain a scanned copy in their electronic investigation file as a record. This will also fulfil disclosure obligations if the matter proceeds to a criminal prosecution.

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

14.5.4 Applicants and AOs must 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

16.1 RIPA for Merton Council CCTV

16.1.1 Directed Surveillance requests for access to Merton 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 targeed covert surveillance (which includes the disclosure of recordings) in the Borough of Merton 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 cameras 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.

16.2 Confidential Information

16.2.1 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 requires particular consideration. Unwarranted access to them during an investigation may be grounds for cancelling the Authorisation.

16.3 Duration of Authorisation

16.3.1 The duration for authorised surveillance is as follows:

a) 3 months for Directed Surveillance ("DS "), or
b) 12 months for a CHIS from grant of Judicial Approval,
c) four months for a juvenile CHIS.

16.4 Reviews

16.4.1 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].

16.4.2 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.

16.5 Renewals

16.5.1 Renewals must take place prior to the authorisation expiring; otherwise, the authorisation will automatically expire in accordance with the surveillance authorisation limits. 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.

16.6 Cancellation

The officer has a duty to request the AO cancel the authorisation, where the authorisation no longer meets the criteria upon which it was originally authorized, for example, a fly-tipping hotstop may be subject to directed surveillance for 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 and Record Keeping

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. These records should be retained for a period of at least 7 years from the ending of the authorisation.

17.2 London Borough of Merton ("LBM")'s CRR of all authorisations is kept and maintained by the Information Governance Team Leader. Please see section 10 regarding the mandatory requirement to complete a RIPA Request Form and to obtain an URN.

17.3 All original applications, reviews, renewals and cancellation forms are to be served by hand, on the Information Governance Team Leader within 5 days of the grant of Judicial Approval, and stored in locked cabinets.

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'. The Council must be ready to provide the relevant witness if authenticity is ever questioned in court.

7.15 Sections 37 to 44 of the Police, Crime, Sentencing & Courts Act (PCSCA) 2022 came into force on 8 November 2022. This provides Merton Council with a further power to extract data held on electronic devices. Before action is taken, there must be a reasonable belief that information stored on the device will be relevant for one of three scenarios and satisfaction that the extraction of the information is necessary and proportionate to achieve the purpose.

7.16 The three scenarios provided under s37 (2) PCSCA are for the purpose of:

(a) preventing, detecting, investigating or prosecuting crime;
(b) helping to locate a missing person; or
(c) protecting a child or an at-risk adult from neglect or physical, mental or emotional harm.

7.17 To ensure any extraction of stored communication under s.37 PCSCA remains lawful, it is essential that the criteria and procedures set out within the PCSCA and the association Code of Practice are fulfilled. A failure to follow these procedures correctly could result in a s.3 Investigative Powers Act (IPA) 2016 offence (unlawful interception) being committed.

17.8 As recommended by the IPCO, the Council will maintain a separate auditable record of any decisions and actions under RIPA which will be available to the SRO for scrutiny and the Investigatory Powers Tribunal ('IPT'),

Page 29

established under Part IV of the 2000 Act, to carry out its functions (see section 11 of the Code of Practice for more information on the IPT).

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 causes of errors, and the implementation of the processes to minimise repetition of errors; (for example, 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
- where necessary, oversight of the implementation of post inspection action plans approved by the IPCO.

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 IPCO. To avoid role conflict, the SRO should never act as an AO.

18.3 Please see Appendix 1 for the current SRO details, who is also a member of the corporate leadership team.

19. RIPA Reviews/Reports

19.1 Given the substantial reduction in the use of RIPA powers since 2015, Merton Council only holds 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 Councillors shall receive an annual report 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 the Standards and General Purposes Committee.

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 online, 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 online world: to which there are rules and 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' online sources (such as Facebook, X, Tiktok, Snapchat, Youtube, WhatsApp 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 via social media to establish or check some basic facts is unlikely to require an authorisation for directed surveillance, 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. 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' online 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 authorisation 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.

20.9 This section should be read in conjunction with the guidance contained in the updated Codes of Practice (links shown below) which offer some helpful examples:

- For Surveillance – see paragraphs 3.10 to 3.17 – CHIS Code (publishing.service.gov.uk)

- For CHIS – see paragraphs 4.29 – 4.35 - CHIS Code draft formatted (publishing.service.gov.uk)

20.10 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 legislation. It should be noted that the information the Council collects about individuals, how it collects it and uses it will have to comply with stricter transparency and accountability rules under Data Protection Act 2018 and General Data Protection Regulation (GDPR). Readers are referred to the Council's Data Protection Policy and all the other related Council Information Governance policies.

21. Training & Monitoring

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 appropriate RIPA training will be provided to relevant staff members every three years. In addition, RIPA updates/ advice notes and briefings will be provided to relevant staff from time to time. However, where staff already receive training as part of their professional accreditation or development, that will be taken into account when assessing their needs.

22. Investigatory Powers Commissioner's Office (IPCO)

22.1 The IPCO is the supervisory body for RIPA and deals with the following:

- requests for RIPA statistical information
- inspections of Local Authorities including Merton Council, usually every 3 years;
- publication of regular reports on RIPA activity.

23. Collaboration with other authorities/agencies

23.1 The Council shall endeavor to conclude written collaboration agreements with any other authorities with whom it works regularly, such as the Police or neighbouring Trading Standards Authorities.

23.2 Prior to any activity, where the Council uses external partners or agents the Council will seek their written acknowledgement that they:

- will act as an agent of the Council
- have seen the written Authorisation for the activity they are undertaking

- will comply with the specific requirements permitted by the Authorisation
- recognise they may be subject to inspection by the IPCO for RIPA activity

24. 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 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.

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 the correct interpretation if you are unsure.

24.4 The three Codes of practice now in force and of concern to the Council (and accessible through the Home Office website) are:

- Covert Surveillance & Property Interference
- Covert Human Intelligence Sources
- Communications data

CHIS Code (publishing.service.gov.uk)

Covert human intelligence sources: draft code of practice - GOV.UK (www.gov.uk)

https://assets.publishing.service.gov.uk/media/641adb48e90e0769f373364e/Communications_Data_Code_of_Practice.pdf

Home Office guidance if provided to local authorities when on seeking judicial approval at https://assets.publishing.service.gov.uk/media/5a7b036640f0b66eab99e4fc/local-authority-england-wales.pdf

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.

25.3 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 purposes 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 information means taking such steps as might be necessary to make access to the data impossible.

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 provides 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.

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 30/04/2018, the IPT awarded £25,000 to reflect the gravity of the breach and damage suffered and a further award of £21,694 in respect of costs, total 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's conclusion was that no authorization could properly have been granted and, if one had been, it would have been 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.

Further advice and or assistance on the Council's RIPA policy and procedures can be obtained from Legal Services.

Contact Details:
David Fellows
Assistant Head of Law
South London Legal Partnership
(in-house legal team to Merton Council)
Tel: 020 8545 4568
David.Fellow@merton.gov.uk

APPENDICES

APPENDIX 1: Senior Responsible Officer (SRO) Contact Details

John Scarborough, Managing Director of South London Legal Partnership, and Monitoring Officer: John.scarborough@merton.gov.uk

APPENDIX 2: List of Authorising Officers and Contact Details

Margaret Culleton – Head of Internal Audit; margaret.culleton@merton.gov.uk; 020 8545 3149

John Bosley – Assistant Director of Public Space Contract and Commissioning; John.Bosley@merton.gov.uk; 020 8545 3190

APPENDIX 3: Senior Enforcement Lawyer

Gary Ward – Senior Lawyer (Enforcement and Licensing); Gary.Ward@merton.gov.uk 020 8274 5242

(The task of identifying relevant offences and advising generally in relation to RIPA and DC may be assigned to other appropriate members of the SLLP Enforcement Team)

APPENDIX 4: Designated Senior Officer's Contact Details

Communications Data Designated Senior Officer: James Armitage, Head of Regulatory Services: James.Armitage@merton.gov.uk; 020 8545 1234

Page 36

Appendix 5 (Annex B: Judicial application/order form)

Application for judicial approval for authorisation to obtain or disclose communications data, to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B.

Local authority:

Local authority department:

Offence under investigation

Address of premises or identity of subject:

Covert technique requested: (tick one and specify details)

Directed Surveillance ☐

Covert Human Intelligence Source ☐

Summary of details

Note: this application should be read in conjunction with the attached RIPA authorisation/RIPA application or notice.

Investigating Officer:

Authorising Officer/Designated Person:

Officer(s) appearing before JP:

Address of applicant department:

Contact telephone number:

Contact email address:

Local authority reference:

Number of pages:

Wimbledon Magistrates' Court

Order made on an application for judicial approval for authorisation to use a covert human intelligence source or to conduct directed surveillance. Regulation of Investigatory Powers Act 2000 sections 23A, 23B, 32A, 32B Magistrates' court.

Having considered the application, I (tick one):

☐ am satisfied that there are reasonable grounds for believing that the requirements of the Act were satisfied and remain satisfied, and that the relevant conditions are satisfied and I therefore approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal of the authorisation/notice.

☐ refuse to approve the grant or renewal and quash the authorisation/notice.

Notes

Reasons

Signed: _____
(Justice of the Peace/District Judge)
Date:
Time:
Full name:
Address of magistrates' court:

Appendix 6: Arrangements for Non-RIPA activity

1. There may be occasions when during the course of an investigation it may become necessary to conduct surveillance of individuals in respect of matters that do not satisfy the crime threshold. For example, in relation to an investigation into an allegation that a contractor is not carrying out their work as contracted, a serious disciplinary offence by a member of staff is alleged e.g. gross misconduct, or children are at risk where Court Orders are not being respected, then a RIPA authorisation is not usually available because criminal proceedings are not normally contemplated.

2. Similarly, there may be serious cases of neighbour nuisance or involving antisocial activity which involve potential criminal offences for which the penalty is below the thresholds which would enable use of a RIPA authorisation. Nonetheless in such cases there may be strong grounds for carrying out directed surveillance or use of a CHIS. Indeed there may be circumstances in which directed surveillance or use of CHIS is the only effective means of efficiently obtaining significant information to take an investigation forward.

3. A person may make a claim or a complaint to the Investigatory Powers Tribunal should they consider the use of directed surveillance or use of a CHIS infringed their Article 8 rights. It would be then for the Council to satisfy the IPT that such infringement was justified, necessary and proportionate in pursuit of a legitimate aim. Completing the Non-RIPA application forms provides a written record of those matters taken into account at that time regarding justification, necessity and proportionality.

4. In these circumstances, the investigating officer is required to go through the RIPA authorisation process in terms of considering: a) Why there is no other alternative to undertaking the directed surveillance; b) Why the surveillance is necessary; and, c) How it is proportionate in the circumstances.

5. The investigating officer is required to complete a ‘non-RIPA’ authorisation form (in the same terms of a RIPA form but clearly marked ‘NON-RIPA’). The application must be submitted to an Authorising Officer for approval.

6. Where it is deemed that the above-mentioned criteria have been satisfied, the non RIPA surveillance should be monitored and reviewed in accordance with the existing Council policy. The same arrangements for RIPA authorisations are followed for Non-RIPA authorisations, that is, a Non-RIPA URN is required; the operation is subject to review and cancellation; and records are retained in the same way and are to be made available to an IPCO, if requested. In the event of a claim or complaint made to the IPT it shall be essential to have such records to demonstrate the activity was justified, necessary and proportionate.

Test purchase exercises

7. If no application for directed surveillance is made in relation to a test purchase exercise involving juveniles the ‘Non RIPA Activity’ procedure shall be followed. On completion of the test purchase exercise a written record shall be made of the review of the exercise, including an assessment of the risks of private

information being obtain and the risk of collateral intrusion. Regard shall be had to the reviews before embarking on successive test purchase exercises.