APPENDIX 1

LONDON BOROUGH OF TOWER HAMLETS

POLICY ON THE USE OF COVERT SURVEILLANCE REGULATION OF INVESTIGATORY POWERS ACT 2000

Jan 2018

CONTENTS

1. Introduction

1.1 The Regulation of Investigatory Powers Act 2000 ("RIPA") provides a statutory framework for public authorities to use covert investigatory techniques such as surveillance, where necessary and proportionate, for the purpose of preventing or detecting crime and disorder. If such activities are conducted by council officers, then RIPA regulates the use of these powers in a manner that is compatible with the Human Rights Act 1998. Surveillance includes; monitoring, observing or listening to persons, monitoring or observing their movements, conversations or their other activities or communications, and the recording of anything monitored, observed or listened to in the course or surveillance. It also includes surveillance by or with the assistance of a surveillance device.

1.2 Part ll of Chapter ll RIPA sets out the provisions in relation to Directed Surveillance. This is covert surveillance that is not intrusive, but is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about an

individual (other than by way of an immediate response to events or circumstances, such that it is not reasonably practicable to seek authorisation under the 2000 Act). Surveillance is covert when the subject of the surveillance is unaware that it is being carried out. The provisions aim to regulate the use of these investigative techniques and to prevent the unnecessary invasion of the privacy of individuals.

1.3 Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in a private vehicle. Local authorities cannot authorise surveillance that is intrusive

1.4 Relevant Officers of the London Borough of Tower Hamlets are authorised in certain circumstances to use RIPA to undertake directed surveillance and access low level communications data in order to detect and prevent crimes such as anti-social behaviour, offences under the trading standards legislation, and fraud. Typical examples of directed surveillance include covertly following people,

covertly taking photographs of them, and using hidden cameras to record their movements

1.5 Whilst RIPA itself does not provide any specific sanction, where an activity occurs which should otherwise have been authorised, any evidence thereby obtained may be inadmissible in court. The activity may also be unlawful under the Human Rights Act 1998 and may result in an investigation by the Ombudsman and/or the Investigatory Powers Tribunal.

1.6 RIPA provides that responsibility for authorising directed surveillance, use of a Covert Human Intelligence Source (CHIS) or acquisition of communication data lies with a Divisional Director, Head of Service, Service Manager or equivalent. RIPA was amended by the Protection of Freedoms Act 2012. Since 1st November 2012 the internal authorisation for such surveillance methods does not take effect until such time as a Magistrate has made an order approving it. The government introduced this requirement to impose a

statutory check on local authorities and to ensure that powers are only used to prevent serious crime.

1.7 This Policy must be read in conjunction with the current Home Office Guidance and relevant Codes of Practice.

1.8 The Council has broad statutory functions and takes targeted enforcement action in relation to those functions having regard to the following –

- The Tower Hamlets Plan
- The Tower Hamlets Strategic Plan
- The Tower Hamlets Local Plan
- Any external targets or requirements imposed under relevant legislation
- The Councils Enforcement Policy

1.9 There may be circumstances in the discharge of its statutory functions in which it is necessary for the Council to conduct directed surveillance for one or more of the following purposes

- Preventing or detecting crime where the offence attracts a maximum custodial sentence of 6 months or more or where the offence relates to the underage sale of alcohol, tobacco and other age related products

- Preventing disorder where the disorder involves a criminal offence punishable by a maximum term of at least 6 months imprisonment, whether on summary conviction or on indictment

1.10. As a consequence of the Protection of Freedoms Act 2012 the council's use of RIPA is restricted to the following offences:

- An offence punishable by a maximum term of at least 6 months imprisonment
- An offence under section 146 of the Licensing Act 2013 (sale of alcohol to children)
- An offence under section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children)
- An offence under section 147A of the Licensing Act 2003 (persistently selling alcohol to children); or
- An offence under section 7 of the Children and Young Persons Act 1933 (sale of tobacco etc. to persons under eighteen)

- An offence under section 141A of the Criminal Justice Act 1988 (sale of knives and certain articles with blade or point to persons under sixteen)
- An offence under Regulation 31 of the Pyrotechnic Articles (Safety) Regulations 2015 (prohibition on making fireworks & other pyrotechnic articles available to persons younger than the minimum age limit)
-

The crime or disorder detected or to be prevented, must meet the crime threshold. The crime threshold came into force on 1st November 2012 and only applies to directed surveillance

Basis for lawful surveillance activity

1.11 The Human Rights Act 1998 gave effect in UK Law to the rights set out in the European Convention on Human Rights (ECHR). Some of these rights are absolute, while others are qualified, meaning that it is permissible for the State to interfere with those rights if certain conditions are satisfied. Amongst the qualified rights is a person's right to respect for their private and family life, home and correspondence, as provided for by article 8 of the ECHR. It is Article 8 that is most likely to be engaged when public authorities seek to obtain private information about a person by means of covert surveillance. Article 6 of the ECHR, the right to a fair trial, is also relevant where a prosecution follows the use of covert techniques, particularly where the prosecution seek to protect the use of those techniques through public interest immunity procedures.

1.12 The Council understands that it is obliged to comply with the provisions of the Regulation of Investigatory Powers Act 2000 ("RIPA") in order to conduct directed surveillance. The

Council believes that by complying with the provisions of RIPA, the Council should also ensure that any directed surveillance comes within the qualification in Article 8(2) of the ECHR and, accordingly, the Council should not breach its obligation under section 6(1) of the Human Rights Act 1998.

1.13 The Investigatory Powers Commissioner's Office (IPCO) has recommended as best practice that public authorities develop a corporate policy. The Council concurs with the OSC that a corporate policy is best practice and has had such a policy in effect since 27th July 2004. This document is the Council's corporate policy in relation to directed surveillance. The Council also has a policy in place in respect of the use of covert human intelligence sources, which is contained in a separate document.

1.14 The Council has prepared guidance notes and a procedure manual on the use of directed surveillance, which should be read with this policy.

2. Responsibilities

2.1 The Divisional Director, Legal Services is responsible for the following –

- Ensuring the proper implementation of this policy and the guidance and procedures that go with it.
- Ensuring the Council complies with the requirements of Part II of RIPA (directed surveillance)
- Ensuring that due regard is given to any code of practice issued pursuant to section 71 of RIPA.
- Engaging with commissioners and inspectors when they conduct inspections under RIPA.
- Overseeing the implementation of any recommendations made by a commissioner.

2.2 The Divisional Director Public Realm and Divisional Director Community Safety are the Council's authorising officers for the purposes of considering applications for authorisation to conduct directed surveillance, with the exception of cases where confidential information is either targeted or likely to be obtained. In these cases the Chief Executive should give authorisation, and in their absence, the person who is their deputy. If the Divisional Director Public Realm or Divisional Director Community Safety are unavailable and the Divisional Director Legal Services agrees that it is appropriate in respect of a specified application, then the Head of Audit and Risk or the Head of Community Safety

may act as the Council's authorising officer in respect of that application.

2.3 The Council considers that applications for authorisation to conduct directed surveillance should be of a high and consistent standard. For this reason, all applications should be cleared by a gate-keeper before consideration by the authorising officer. The Council's gate-keeper is the Head of Community Safety. In the absence of that officer, the Intelligence Team Leader, Risk Management & Audit may act as Gatekeeper although they must not act as the authorising officer for an application where they have been the gatekeeper..

2.4 All officers have responsibility to ensure that directed surveillance is only conducted where there is an authorisation from the authorising officer and a Justice of Peace has approved the authorisation.

3. Directed Surveillance

3.1 Terms used in this policy have the meanings given by RIPA or any relevant code of practice made under section 71 of RIPA.

3.2 Directed surveillance is surveillance which is covert (i.e. secret) but not intrusive, that is, it takes place other than in residential premises or private vehicles, and is undertaken:

- for the purposes of a specific investigation or a specific operation
- in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and
- it is conducted otherwise than by way of an immediate response to events or circumstances, the nature of which is such that it would not be reasonably practicable for an authorisation under Part II of RIPA to be sought for the carrying out of the surveillance
- The surveillance must only be carried out for the purpose of preventing or detecting a criminal offence punishable by a maximum term of at least 6 months imprisonment

3.3 Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle. It involves the presence

of an individual inside the premises or in the vehicle, or is carried out by means of a surveillance device. Surveillance equipment mounted outside the premises will not be intrusive, unless the device consistently provides information of the same quality and detail as might be expected if they were in the premises/vehicle, e.g. by means of a zooms lens. The Council is not permitted to conduct intrusive surveillance under RIPA and so will not use intrusive surveillance.

4. Priorities

4.1. The Council will use directed surveillance where an authorisation has been obtained under RIPA, and only in accordance with the terms of the authorisation and where a Justice of the Peace has approved the authorisation.

4.2. An authorisation may only be granted where

- it is necessary for one of the following purposes: (1) preventing or detecting crime; (2) preventing disorder;
- It complies with any additional conditions imposed by the Secretary of State under RIPA. From 1 November 2012 this means that the Councils use of RIPA is restricted to the following offences:
- An offence punishable by a maximum term of at least 6 months of imprisonment;
- An offence under section 146 of the Licensing Act 2003 (sale of alcohol to children);
- An offence under section 147 of the Licensing Act 2003 (allowing the sale of alcohol to children)
- An offence under section 147A of the Licensing Act 2003 (persistently selling alcohol to children); or
- An offence under section 7 of the Children and Young Persons Act 1933 (sale of tobacco etc. to persons under eighteen)
- An offence under section 141A of the Criminal Justice Act 1988 (sale of knives and certain articles with blade or point to persons under sixteen)

- An offence under Regulation 31 of the Pyrotechnic Articles (Safety) Regulations 2015 (prohibition on making fireworks & other pyrotechnic articles available to persons younger than the minimum age limit)

The action proposed must be necessary and proportionate and approved by a Justice of the peace

4.3. Having regard to the permitted purposes and to the requirements in the Council's Enforcement Policy that enforcement action should be targeted (to the Council's stated objectives), the Council's current priorities for the use of RIPA are –

- Anti-social behaviour
- Underage sales of knives, tobacco, alcohol and fireworks
- Detecting and preventing Fraud, including misuse of disabled parking badges
- Unlawful street trading of tobacco
- Breach of Premises License conditions including touting
- Bribery Act offences

5. Authorisations

5.1 Prior to directed surveillance taking place RIPA provides that the surveillance must be authorised by the councils authorising officer as defined in section 2 of this policy and approved by a justice of the peace

5.2 Surveillance can only take place where it is for the purpose of preventing or detecting crime or of preventing disorder where the crime threshold is met and relates to an offence of the kind specified in paragraph 4.3 above. The authorisation and approval must ensure that the surveillance is both necessary and proportionate as well as limiting any potential collateral intrusion. Further the authorisation will need to consider whether confidential information is likely to be obtained as a result of the covert surveillance. Confidential information includes confidential personal information.

5.3 The Council is committed to only using directed surveillance in accordance with RIPA and the Code of Practice. The Council has adopted a guidance manual to assist officers to make applications and grant authorisation in accordance with RIPA and the Code. The Council will have regard to the most recent relevant Code of practice. The current Code came into force on 20 September 2018.

Procedure for authorising

5.4 The Council is committed to achieving a consistent high standard in applications for authorisation to conduct directed surveillance. All applications must first be submitted to the Council's gatekeeper as specified in section 2 of this Policy. Only when the gatekeeper has cleared the application may the authorised officer consider it.

5.5 Matters for the Authorising Officer to consider:

- The type of offence – Consider whether the application passes the crime threshold

- Necessity and proportionality -The 2000 Act first requires that the person granting an authorisation must believe that the authorisation is **necessary** in the circumstances of the particular case under section 28(3) (b) of RIPA. Once necessity is established then proportionality must be considered. Officers seeking an authorisation under the RIPA 2000 Act should ensure that there is a justifiable interference with an individual's Article 8 rights, i.e. it is necessary and **proportionate** for those activities to take place, and there is no less intrusive means of achieving the same aim.

The following elements of proportionality should be considered:

- Balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

- 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 necessary result;

- Evidencing, as far as reasonably practicable, what other methods have been considered and why they were not implemented

5.6 The above involves balancing the intrusiveness of the activity on the target subject and others who might be affected by it, against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances. Each case will be judged on and be unique on its merits. Consideration should be given to whether the information which are sought, could reasonably be obtained

by other less intrusive means. All such activity must be carefully managed to meet the objective in question.

When setting out the proportionality of the surveillance, it is important that the applications include clear statements of the other reasonable possible methods of obtaining the desired information and the reasons why they have been rejected. This approach will also apply, equally to arguments for the necessity of surveillance.

5.7 Before authorising surveillance the Authorising Officer should take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be taken, wherever practicable to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation. Those carrying out the surveillance should inform the Authorising Officer if the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation. As part of the process an assessment should be made of the risk of what is termed “collateral intrusion”. If collateral intrusion is inevitable, publication of the material/evidence obtained must be carefully controlled. If the evidence is used in court proceedings, it may be possible to deal with collateral intrusion by editing.

5.8 The authorising Officer should be aware of sensitivities in the community to any directed surveillance.

5.9 The authorising Officer should be aware of similar activities being undertaken by other public authorities.

5.10 The Authorising Officer should have regard to the current Code of Practice

5.11 All authorisations are required to have a Unique Reference Number ("URN") and the officer seeking the authorisation must obtain the URN from Legal Services at the time of preparing the application (i.e. prior to seeking authorisation) and the authorising officer should not authorise that authorisation unless a URN has been provided.

5.12 After the Council's authorising officer has authorised the directed surveillance, they must immediately notify the Divisional Director Legal Services or nominee who will update the central record and make the necessary court application to obtain approval from a justice of the peace.

Magistrates Approval

5.13 Approval can only be given if the Magistrate is satisfied that:

a) There were reasonable grounds for the authorising officer believing that the directed surveillance or deployment of a CHIS was necessary and proportionate and that there remains reasonable grounds for believing so

b) The authorising officer was of the correct seniority within the organisation, that is, a Divisional Director, Head of Service, Service Manager or equivalent
c) The granting of the authorisation was for the correct purpose, that is, preventing and detecting crime and disorder and satisfies the serious offence test (crime threshold)
d) Any other conditions set out in any order under Part 2 of RIPA are satisfied

No investigation may commence unless and until a Justices approval has been obtained.

5.14 Written authorisation may be given by the authorising Officer for 3 months

6 Duration/Review/Renewal

6.1 An authorisation for directed surveillance lasts for 3 months before having to be renewed. When authorising directed surveillance, the authorising officer is required to set a date for review of that authorisation. This is known as the first review. The Code of Practice requires regular reviews be undertaken by the authorising officer to assess the continuing need for the surveillance. The frequency of reviews must be considered at the outset by the authorising officer. Reviews should take place as frequently as is considered necessary and practicable, on a case by case basis. This frequency should increase where the surveillance is providing access to confidential material or involves collateral intrusion.

6.2 Authorisation forms do not expire, they must be reviewed, renewed, where necessary (by application to the court) or cancelled once they are no longer required, whether the surveillance is conducted or not.

6.3 During a review, the authorising officer who granted or last renewed the authorisation may amend specific aspects of the authorisation, for example, to cease surveillance against one or a number of named subjects or to discontinue the use of a particular tactic.

6.4 Authorisation for renewal is required to be approved by a Justice of the Peace at the Magistrates Court. Where applicable Authorisations should be renewed on application to the Court before the maximum period in the authorisation has expired. The Authorising Officer must consider the matter afresh including taking into account the benefits of the surveillance to date, and any collateral intrusion that has occurred. This will need to be explained to the Justice of the Peace. An authorisation cannot be renewed after it has expired.

7 Cancellations

7.1 If on a review, the authorising officer is satisfied that the authorisation is no longer necessary on the ground under which it was granted or renewed, or it is no longer proportionate to what is sought to be achieved by carrying it out, then the authorising officer must request that the authorisation be cancelled and no further surveillance under that authorisation is to be carried out.

7.2 The date the authorisation was cancelled should be centrally recorded and documentation of any instruction to cease surveillance should be retained. On cancelling a directed surveillance authorisation, it is good practice to keep a record detailing the product obtained from the surveillance and whether or not objectives were achieved, although there is no requirement to do so.

8. Retention and destruction of product surveillance

8.1 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements, or for a suitable period, and be subject to review. There is nothing in RIPA which prevents material obtained from properly authorised surveillance from being used in other investigations. Authorising Officers must therefore ensure that they follow the procedures for handling, storage and destruction of material obtained through the use of covert surveillance. Authorising Officers must also ensure compliance with the appropriate data protection requirements.

9. Combined Authorisations

9.1 From time to time, it may well be that the directed surveillance will be undertaken by a Covert Human Intelligence Source ("CHIS"). If it does, then both actions must be authorised. A single authorisation can combine the two, however, and this should be done on the application form used for the authorisation of the CHIS.

10. Security of Covert Technical Equipment

10.1 The Council also requires each Service that uses covert technical equipment when undertaking surveillance to ensure that such equipment is securely locked away when not used. Further, such equipment will only be issued to an officer who has authorisation to use it. There will be a logging in and out book and the officer will be required to sign for the equipment. In signing for the equipment, the officer will be reminded that misuse of the equipment is a disciplinary offence.

11. Communications Data

11.1 Communications data is information held by communication service providers (for example, telecommunications, and postal companies). The Act makes provision for obtaining communications data from such service providers and the disclosure to any person of such data. The RIPA (Communications Data) Order 2003 came into force in January 2004. It allows Local Authorities to acquire limited information in respect of subscriber details and service data. It does not allow Local Authorities to intercept, record or otherwise monitor communications data, or access the content of communications data.

11.2 Communications data is the “who”, “when” and “where” communication but not the “what”. It is broadly split into 3 categories: “traffic data” i.e. where a communication was made from, to whom and when; “service data“ i.e.. the use made of the service by any person e.g. itemised telephone call records (numbers called), itemised records of connections to internet services; “subscriber data” i.e.. any other information that is held or obtained by an operator on a person that they provide a service to e.g. who is the subscriber, to a particular telephone number, or who is the account holder of an email account, information about the subscriber to a PO Box number.

11.3 Under RIPA Local Authority can only authorise the acquisition of the less intrusive types of Communication data: service use and subscriber information. Under no circumstances can Local Authorities be authorised to obtain traffic data under RIPA. Local authorities are not permitted to intercept the content of any persons communications and it is an offence to do so without lawful authority.

11.4 Communications data can only be obtained for the sole purpose of the prevention or detection of crime and/or disorder. Further, the test of necessity must be met before data is obtained. The conduct involved in obtaining the communications data must be proportionate to what is sought to be achieved, and the risk of collateral intrusion must be considered.

11.5 Material cannot be obtained until a Justice of the Peace has granted approval. Authorisations and notices are valid for a period of one month from the date of the judicial approval.

11.6 Communications data can be accessed using two different methods:-

- The granting of Authorisations, or
- The service of notices

11.7 An Authorisation would allow the Council to collect or retrieve the data itself from the service provider. A notice is

given by the Council to a postal or telecommunications operator and requires that operator to collect the data and provide it to the council.

11.8 Integral to the acquisition of communication data under RIPA is the single point of contact (SPoC). The role of the SPoC is to enable and maintain effective cooperation between a public authority and communication service providers in the lawful acquisition and disclosure of communications data.

11.9 Any notice of authorisation must be passed to the service provider through a SPoC. The Council currently uses National Anti-Fraud Network (NAFN) as its single point of contact. The NAFN provides a SPoC service to local authorities, precluding each authority from the requirement to maintain their own trained staff. Local Authorities using the SPoC at NAFN will still be responsible for submitting any applications to the JP and a designated person in the Local Authority is still required to scrutinise and approve any applications. The Local Authority's designated person is the Council's authorising officer for covert surveillance. The Local Authority investigator (i.e. the applicant) will then submit the relevant judicial application and supporting documents to the JP. The JP will then record its decision on the judicial application form and the local authority investigator will upload a copy of the order to the NAFN SPoC. The NAFN SPoC will then require the communication

data on behalf of the Local Authority in an efficient and effective manner.

12. Central Recording

12.1 A central register of all Authorisations, Reviews, Renewals, Cancellations and Rejections will be maintained and monitored by the Divisional Director Legal with regards to Directed Surveillance and CHIS.

12.2 The Council is required to keep records in relation to authorisations centrally. Those records will be maintained by Legal Services.

12.3 The relevant authorising officer must provide copies of all authorisations and all reviews, renewals and cancellations to the Divisional Director, Legal, or a person nominated by either of them. The authorisation officer must provide those documents forthwith i.e. within a week following signing by the authorising officer.

12.4 The Council will retain records for a period of at least three years from the ending of the authorisation. The Investigatory Powers Commissioner's Office (IPCO) may audit/review the Council's policies and procedures, and individual authorisations, Reviews, Renewals, cancellations and Rejections.

12.5 The documents to be stored will include:-

- A copy of the Forms together with any supplementary documentation and notification of the approval given by the Authorising Officer and the Magistrates Court
- The date and time when any instruction was given by the Authorising Officer
- A record of the period over which the surveillance has taken place
- The frequency of reviews prescribed by the Authorising Officer
- A record of the result of each review of the authorisation
- A copy of any renewal of any authorisation, together with the supporting documentation submitted when the renewal was requested
- The unique reference number (URN) for the authorisation
- A record of the date of the cancellation of the authorisation

12.6 All officers are expected to use the most up to date versions of forms recommended by the Home Office.

13. Training

13.1 Authorising officers can only authorise, once they have undertaken training on the operation of RIPA and the Code of Practice. The Council's gatekeepers may only clear applications for consideration by the authorising officer after undertaking the same training as the authorising officers.

13.2 All officers who may seek to use directed surveillance during an investigation must also have undertaken training on the operation of RIPA and the Code of Practice.

13.3 The Council will arrange appropriate training courses at regular intervals. It is expected that members of the Corporate Leadership Team will require authorising officers, gatekeepers and those who may apply to conduct directed surveillance to undertake the training.

14. Member oversight

14.1 The Council's Standards Committee will review this Policy and have oversight of the Council's conduct of directed surveillance. If issues arise, the Standards Committee will make recommendations to Cabinet for action.