


Non-Executive Report of the:  <b>Audit Committee</b>  7 <sup>th</sup> April 2021	
<b>Report of:</b> Janet Fasan, Divisional Director of Legal & Interim Monitoring Officer	<b>Classification:</b> Open (Unrestricted)
<b>RIPA Policy 2021</b>	

<b>Originating Officer(s)</b>	Agnes Adrien, Head of Litigation, Legal Services
<b>Wards affected</b>	(All Wards);

## Executive Summary

On 24 April 2019, Cabinet agreed a council-wide Enforcement Policy. The Enforcement Policy is concerned with the Council's exercise of its criminal and quasi-criminal enforcement functions. The policy is also concerned with offences and contraventions of legislation that fall within the Council's responsibility to enforce.

This report details proposed amendments to the Regulatory Investigatory Powers Act ("RIPA") Policies for directed surveillance, the use of covert human intelligence sources which accompany the Council's Enforcement Policy. It is also proposed that a RIPA Social Media Policy is introduced.

The policies are being reviewed to take account of changes in legislation and good practice.

## Recommendations:

The Audit Committee is recommended to:

1. Consider and comment on the proposed amendments to the RIPA policy and the introduction of the Social Media policies at Appendices 1 and 2.

## 1. REASONS FOR THE DECISIONS

- 1.1 The Council's policies need to reflect changes to legislation and good practice, and to be reviewed annually to be both relevant and up to date. Going forward, in line with recommended practice, the Audit Committee will receive an annual report summarising any policy changes and use of directed

surveillance and covert human intelligence sources.

## **2. ALTERNATIVE OPTIONS**

- 2.1 The Council can choose not to update its RIPA Policy or introduce the RIPA Social Media Policy but it may mean that formal enforcement action taken by officers fails. There is also a risk of unauthorised covert surveillance taking place.

## **3. DETAILS OF THE REPORT**

- 3.1 These Policies are being reviewed and revised to take account of changes in legislation and to ensure that council officers use social media in a controlled and auditable manner. The intention of the revised RIPA policy and the introduction of a RIPA Social Media Policy is to ensure that there is a consistent approach to the use of RIPA throughout the council.
- 3.2 The revised RIPA Policy takes account of the principles set out in the Covert Surveillance and Property Interference Revised Code of Practice and the Covert Human Intelligence Sources Revised Code of Practice.
- 3.3 **Amendments to the Policy**  
It is necessary to update the Council's current RIPA Policy as there have been various changes in procedure and legislation that have taken place that need to be reflected in the refreshed policy.
- 3.4 The suggested changes to the council wide RIPA policy include the following:
- a) Extending the authorisation period for juveniles from one to four months.
  - b) Defining what constitutes confidential information (i.e. legally privileged material, journalistic material, constituency business of MPs and finally confidential personal information relating to physical or mental health or spiritual counselling)
  - c) The introduction of the Investigatory Powers Act 2016 came into force on 11 June 2019. Acquisitions of communications data by a local authority no longer requires judicial approval by a magistrate. An authorising officer in the Office for Communications Data Authorisations (OCDA) can authorise any lawful request for any of the specified purposes.
  - d) The introduction of a RIPA Social Media Policy, which will ensure that there is a consistent approach to the use of social network sites for intelligence gathering and/or as a surveillance tool. Auditable records should be retained when activity is carried out on the internet in a way in which staff may interact with others using public open websites e.g. social networking services or private exchanges where the party may not reasonably be expected to know their identity. Managers are expected to regularly review the internet activity of their teams and maintain records.

### 3.5 Current RIPA Policy

There are two RIPA Policies appended to the Council-wide Enforcement Policy. One relates to Directed Surveillance and the other one covers Covert Human Intelligence Sources. For activities under RIPA, this means that before obtaining or disclosing communications data under Part 1 of RIPA or conducting covert surveillance or using a covert human intelligence source under Part 2 of RIPA, the Council will require its own authorisation to be approved by a justice of the peace. This adds an extra layer of approval. The requirement for judicial approval to conduct covert surveillance, or use a covert human intelligence source, under Part 2 of RIPA came into force on 1 November 2012.

### 3.6 Extending Authorisations for Juveniles

The Secretary of State made the Amendment of the Regulation of Investigatory Powers (Juveniles) Order 2000 which came into force 20 July 2018. The order extended the period permitted for a juvenile's authorisation from one to four months.

### 3.7 Defining Confidential Information

Where a Covert Human Intelligence Source (CHIS) is targeted to obtain confidential information or confidential information is likely to be obtained, the Chief Executive is the Authorising Officer, rather than the Divisional Director of Public Realm or Community Safety. Defining confidential information in the policy provides clarity to the Gatekeeper in making a decision as to who the Authorising Officer is.

### 3.8 Interception of communications

The Investigatory Powers Act 2016 ("IPA") came into force on 11 June 2019. This is the main legislation governing the acquisition of communications data. The interception of communications is regulated by the Office for Data Communication Authorisation (OCDA).

3.9 Communications data is information about communications: the 'who', 'where', 'with whom' and 'how' of a communication but not the content i.e. Not what was actually said or written. It is the communication that can be acquired. E.g. if during a Council investigation into criminal activity, who a particular mobile telephone was registered to was required, this information could be obtained. This would be communications data.

3.10 The acquisition of communications data by local authority officers is no longer subject to judicial approval by a magistrate. There is a requirement for a local authority making an application to ensure that someone at least the rank of Service Manager is aware that the application is being made before it is submitted to OCDA. An authorising officer in OCDA can authorise any lawful request for any of the specified purposes from any listed public authority.

### 3.11 Social Media

Information that is available online, presents opportunities for public authorities to view or gather information which may assist them in preventing

or detecting crime. The internet can be used for intelligence gathering and/or as a surveillance tool by officers in the course of their duties.

- 3.12 The introduction of a RIPA Social Media Policy will ensure that there is a consistent approach to the use of social network sites for intelligence gathering and/or as a surveillance tool. A preliminary examination of social media to establish whether the site or its contents are of interest is unlikely to interfere with a person's reasonable expectation of privacy and is unlikely to require a directed surveillance authorisation.
- 3.13 When researching "open source" material this would not generally require authorisation. "Open source" relates to materials that can be viewed on social media without the need to become a subscriber, follower or friend. However, return visits to build up a profile could alter the position as it could constitute directed surveillance depending on the circumstances.
- 3.14 Important points to note when accessing social media sites are as follows:
- i. Where on-line monitoring or investigation is conducted covertly or for the purpose of a specific investigation or operation it is likely to result in obtaining private information about a person or group. An authorisation should be considered in these circumstances.
  - ii. Where a person acting on behalf of a public authority is intending to engage with others without disclosing their identity, a Covert Human Intelligence Source (CHIS) authorisation may be required.
  - iii. Officers should not use a false identity to disguise on-line activities. The use of a false identity should not be used for a covert purpose without authorisation.
  - iv. auditable records are to be retained when activity is carried out on the internet in a way in which staff may interact with others using public open websites e.g. social networking services or private exchanges where the party may not reasonably expected to know their identity. Managers are expected to regularly review the internet activity of their teams and maintain records.

#### **4. EQUALITIES IMPLICATIONS**

- 4.1 An equalities impact assessment will be carried out following the Audit Committees comments on the policy.

#### **5. OTHER STATUTORY IMPLICATIONS**

- 5.1 This section of the report is used to highlight further specific statutory implications that are either not covered in the main body of the report or are required to be highlighted to ensure decision makers give them proper consideration.

- 5.2 Best Value: The report assists with the regularising decision-making in areas in which the Council is already active. The RIPA policy seeks to ensure that covert surveillance is targeted to the Council's policy objectives. This is likely to lead to efficient enforcement action rather than a less-controlled enforcement effort.
- 5.3 Environmental: The Enforcement policy which the RIPA Policy is attached to seeks to support the strategic plan which promotes and improves the economic, social and environmental wellbeing of Tower Hamlets. The extent that the Enforcement Policy aligns enforcement action with the Strategic Plan will tend to promote sustainable action for the environment.
- 5.4 Risk Management: Enforcement action has a variety of inherent risks, including the potential for over or under-enforcement, discrimination, adverse cost orders and damage to the Council's reputation. The principles of enforcement contained in the policy provide a sound basis for decision making that will reduce the likelihood of any adverse outcomes.
- 5.5 Crime reduction and Safeguarding: Enforcement in its broadest sense acts as a deterrent for crime and will therefore likely reduce all form of crime within the Borough. The Enforcement Policy sends a clear message to the perpetrator whilst supporting the victim, that the Council will undertake enforcement where necessary.

## **6. COMMENTS OF THE CHIEF FINANCE OFFICER**

- 6.1 This is a report of the proposed revised policies on the use of covert surveillance and the use of covert human intelligence sources under the Regulation of Investigatory Powers Act 2000. The introduction of a RIPA Social Media Policy is also proposed.
- 6.2 There are no financial implications arising from the recommendations in this report however the RIPA policies are designed to meet the Council's requirements to minimise the risk of fraud, error and omission to Council's services, finances and assets.

## **7. COMMENTS OF LEGAL SERVICES**

- 7.1 The Council is obliged to have regard to the Covert Human Intelligence Sources Revised Code of Practice (August 2018) and the Covert Surveillance and Property Interference Code of Practice (August 2018) in accordance with Part II of the Regulation of Investigatory Powers Act 2000 when seeking to undertake covert surveillance, this includes surveillance by the use of social media.
- 7.2 Although, the preparation and publishing of the policy is not in itself a legal requirement. If the Council does not adopt a revised RIPA Policy and there is no common reference point, there is a risk that covert surveillance is inconsistently applied across different service areas. This might increase the

risk of legal challenge and reduce the fairness and effectiveness of the Council's approach to covert surveillance. The adoption of a policy is considered to be best working practice and will also assist the Councils to demonstrate that it has regard to the Codes of Practice.

- 7.3 Paragraphs 3.8 to 3.9 of the report makes reference to the obligations in the Investigatory Powers Act 2016. The Investigatory Powers Tribunal has jurisdiction to investigate and determine complaints against public authority use of investigatory powers.
- 7.8 The Council must have due regard to the Public Sector Equality Duty under the Equality Act 2010 when carrying out any functions including developing any policies that may have any effect on any protected persons, in particular the duty to eliminate discrimination, harassment and victimisation and advance equality of opportunity and fostering good relations.
- 7.9 The Council also have a duty under the Human Rights Act 1998, when carrying out any function, not to act incompatibly with rights under the European Convention for the Protection of Fundamental Rights and Freedoms.

---

## **Linked Reports, Appendices and Background Documents**

### **Linked Report**

- None.

### **Appendices**

- Appendix A – RIPA Policy – Covert Surveillance
- Appendix B – RIPA Policy – Covert Human Intelligence Source
- Appendix C – Social Media Policy

### **Local Government Act, 1972 Section 100D (As amended)**

#### **List of “Background Papers” used in the preparation of this report**

List any background documents not already in the public domain including officer contact information.

- None.

#### **Officer contact details for documents:**

Agnes Adrien, Head of Litigation, Legal Services

[Agnes.adrien@towerhamlets.gov.uk](mailto:Agnes.adrien@towerhamlets.gov.uk)