
**Regulation of Investigatory Powers Act 2000
Bi-Annual Performance Report January 2019 – June 2019**

Report of the City Barrister and Head of Standards

1. Purpose of the Report

The report advises on the performance of The Council in authorising Regulatory Investigation Powers Act (RIPA) applications, from 1st January 2019 to 30th June 2019.

2. Summary

2.1 The Council applied for 0 Directed Surveillance Authorisations and 0 Communications Data Authorisations in the period above.

3. Recommendations

The Committee is recommended to:

3.1 Receive the Report and note its contents.

3.2 Adopt the revised Surveillance Policy.

3.3 Make any recommendations or comments it sees fit either to the Executive or to the City Barrister and Head of Standards.

4 Report

4.1 The Council has applied for 0 Directed Surveillance Authorisation and 0 Communications Data Authorisations in the first half of 2019.

4.2 The Investigatory Powers Commissioner inspected the Council in March 2019 and the Council was found to demonstrate compliance. The findings are attached as Appendix A.

4.3 In June 2019, the Head of Information Governance & Risk attended a training session hosted by the National Anti-Fraud Network on the Investigatory Powers Act 2016.

- 4.4 The Data Retention and Investigatory Powers Act 2014 (DRIPA) had previously been introduced as an emergency piece of legislation, produced in response to the CJEU decision on data retention. The Investigatory Powers Act 2016 replaced DRIPA and extended beyond the retention of data to the interception of communications, the request for communications data, equipment interference, bulk warrants for communications data and technical capability notices.
- 4.5 Local Authorities have limited powers under the Investigatory Powers Act 2016 e.g. they cannot acquire internet data or interfere with equipment.
- 4.6 The latest changes to come into force under the Investigatory Powers Act 2016 from June 2019 allow local authorities to apply for both event data (data that identifies or describes events) and entity data (data that associates or links people, identifies people e.g. tracing a mobile telephone number to a subscriber).
- 4.7 The introduction of the Office for Communications Data Authorisations (OCDA) means the acquisition of communications data by local authority officers is no longer subject to judicial approval by a magistrate or sheriff.
- 4.8 There is a requirement for a local authority making an application to ensure someone of at least the rank of the Service Manager is aware the application is being made before it is submitted to OCDA.
- 4.9 Entity data no longer needs to meet a minimum crime threshold. For events data, the crime must be a serious crime (See Appendix B).
- 4.10 The recommendations from the Investigatory Powers Commissioner's inspection, and the changes due to the Investigatory Powers Act 2016, have been incorporated into a revised Surveillance Policy. Committee members are asked to adopt the revised policy (Appendix C).

5. Financial, Legal Implications

5.1 Financial Implications

There are no financial implications arising directly from this report, although the Council could incur legal costs should procedures not be correctly followed – Colin Sharpe (Head of Finance) ext. 37 4081.

5.2 Legal Implications

There are no legal implications arising directly from this report, although the Council could incur legal costs should procedures not be correctly followed – Kamal Adatia (City Barrister and Head of Standards) ext. 37 1402.

6. Other Implications

OTHER IMPLICATIONS	YES/NO	Paragraph References Within Supporting Information
Equal Opportunities	No	
Policy	No	
Sustainable and Environmental	No	
Climate Change	No	
Crime and Disorder	No	
Human Rights Act	Yes	HRA Article 8 must be considered for all applications
Elderly/People on Low Income	No	
Risk Management	No	

7. Report Author / Officer to contact:

Lynn Wyeth, Head of Information Governance & Risk, Legal Services
- Ext 37 1291

4th July 2019