

Report to: Audit and Governance Committee

Date: 6 March 2019

Title: Internet and Social Media Research and Investigations – Policy and Procedure

Report of: Assistant Director of Legal & Democratic Services

Ward(s): All

Purpose of report: To seek approval of the Council’s policy on conducting internet and social media research and investigations; and to seek authority for creating and issuing an associated procedure

Officer recommendations: That the Audit and Governance Committee –

- (1) approve Eastbourne Borough Council’s Internet and Social Media Research and Investigations Policy set out in draft at Appendix 1; and
- (2) grant delegated authority to the Director of Service Delivery to develop, implement and ensure compliance with an Internet and Social Media Research and Investigations Procedure for Eastbourne Borough Council

Reasons for recommendations: To ensure the Council has a policy and procedure for the conduct of internet and social media research and investigations that is lawful and ethical

Contact Officer(s): Name: Oliver Dixon
Post title: Senior Lawyer and RIPA Monitoring Officer
E-mail: oliver.dixon@lewes-eastbourne.gov.uk
Telephone number: (01323) 415881

1 Introduction

- 1.1 Home Office guidance on local authority use of covert surveillance states “Elected members of a local authority should review the authority’s use of ...the 2000 Act [*Regulation of Investigatory Powers Act 2000 – “RIPA”*] and set the policy at least once a year.”
- 1.2 This recommendation is reflected in Eastbourne Borough Council’s Policy Statement on the Use of Covert Surveillance, which provides that “the operation of this policy shall be overseen by the Council’s Audit and Governance Committee by receiving reports every 12 months on the policy and its implementation.”

- 1.3 The Council's existing Policy Statement on Covert Surveillance remains valid but needs supplementing with a stand alone policy dealing specifically with online covert activity.

2 Online Covert Activity

- 2.1 The growth of the internet, and the extent of the information that is now available online, presents new opportunities for the Council to view or gather information which may assist its officers in preventing or detecting crime or carrying out other statutory functions, as well as in understanding and engaging with the public it serves. It is important that the Council is able to make full and lawful use of this information for its statutory purposes. Much of it can be accessed without the need for RIPA authorisation; use of the internet prior to an investigation should not normally engage privacy considerations. But if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, RIPA authorisations may need to be considered.
- 2.2 The internet may be used for intelligence gathering and/or as a surveillance tool. Viewing a person's social media site may be required in order to gather information prior to and/or during an operation, an investigation, research or other forms of case review or assessment. For example, officers may seek to obtain such information when following up unpaid Council Tax or business rates debts, assessing applications for Housing Benefit or social housing, seeking to confirm the identity of a resident or claimant, or trying to establish the whereabouts of a tenant.

3 Policy and procedure on conducting internet and social media research and investigations

- 3.1 To avoid unlawful intrusion of privacy, it is important that the Council has, and enforces, a policy on conducting internet and social media research and investigations.
- 3.2 To this end, it is recommended that the Committee approve the policy set out in draft at Appendix 1.
- 3.3 To support the policy, it is further recommended that the Committee grant delegated authority to the Director of Service Delivery to develop, implement, and ensure compliance with a technical procedure for carrying out internet and social media research and investigations. The procedure will include the authorisation process that officers must follow before using the internet in a way that may interfere with a person's privacy.

4 Policy Review

- 4.1 The Committee has responsibility for keeping the policy under review by monitoring it annually (and more frequently if circumstances require). Accordingly, officers would bring a report to Committee at these intervals with information on how the policy has been rolled out and adhered to.

5 Financial appraisal

- 5.1 The Council needs to provide relevant officers with training on the policy and procedure covered by this report. An external training course was delivered to a number of caseworkers and specialist advisors in January 2019, and further training may be required, including at managerial level, once the technical procedure is in place. The cost of this would have to be met from departmental training budgets.

6 Legal implications

- 6.1 The legal framework for online covert activity is referred to in the draft policy and consists principally of the Regulation of Investigatory Powers Act 2000, the Human Rights Act 1998 and data protection legislation. The policy recommended in this report will, if implemented and followed, reduce the Council's exposure to potential liability in respect of any of these legal obligations.

Lawyer consulted 02.01.19

Legal ref: 007697-JOINT-OD

7 Risk management implications

- 7.1 Carrying out internet and social media research and investigations without regard to relevant legislation and codes of practice would expose the Council to the risk of legal liability and reputational loss. To mitigate such risk, it is important for the Council to adopt and roll out the policy and procedure recommended in this report.

8 Appendices

- Appendix 1 – Draft Internet and Social Media Research and Investigations Policy

9 Background papers

The background papers used in compiling this report were as follows:

- Code of Practice on Covert Surveillance and Property Interference (*Home Office, August 2018*) – in particular the provisions dealing with Online Covert Activity at paragraphs 3.10 to 3.17
- Eastbourne Borough Council Policy Statement on Use of Covert Surveillance