STRONGER together

Lewes District Council

EASTBOURNE Borough Council

Working in partnership with **Eastbourne Homes**

| | |
|---|---|
| **Document name:** | Internet & Social Media Research and Investigations Policy |
| **Document type:** | Policy |

| | |
|---|---|
| **Authority(ies) covered:** | Lewes District Council |
| **Responsible (Executive Lead):** | Cllr Andy Smith |
| **Accountable (Operational Lead):** | Oliver Dixon<br>Senior Lawyer and RIPA Monitoring Officer |
| **Version (e.g. first draft, final report):** | 1.0 (final) |
| **Approved by:** | Audit & Standards Committee |
| **Date of publication:** | 22 January 2019 |
| **Revision due:** | January 2020 |

## Contents



## 1. Introduction

1.1 Online open source research is widely regarded as the collection, evaluation and analysis of material from online sources available to the public, whether by payment or otherwise, to use as intelligence and evidence.

1.2 The use of online open source internet and social media research is a method of obtaining information to assist Lewes District Council ("LDC") with its regulatory and enforcement functions. It can also assist with service delivery issues. However, the use of the internet and social media is constantly evolving and with it the risks, particularly regarding breaches of privacy and other operational risks.

1.3 As a public authority, LDC is subject to the Human Rights Act 1998 ("HRA") and, as such, must respect the right of individuals to their private and family life – their 'Article 8' right. This privacy obligation applies to everything the Council does, including research and investigations carried out using the internet. The HRA permits a public authority to interfere with a person's right to privacy *only* in accordance with the law and where doing so is necessary on specified grounds, including the prevention of crime.

1.4 Researching, recording, storing, and using open source information regarding a person or group of people must be both necessary and proportionate and take account of the level of intrusion against any person. The activity may also require authorisation and approval by a magistrate under the Regulation of Investigatory Powers Act 2000 ("RIPA"). To ensure that any resultant interference with a person's Article 8 right is lawful, the material must, in addition, be processed in accordance with the General Data Protection Regulation ("GDPR") and Data Protection Act 2018 ("DPA").

## 2. Scope of Policy

2.1 The objective of this policy and associated procedure is to ensure that all online research and investigations are conducted lawfully and ethically. It

provides guidance to officers about the implications and legislative framework associated with online internet and social media research. The policy also seeks to ensure that the activity undertaken, and any evidence obtained, will stand scrutiny in any subsequent criminal proceedings.

2.2 This policy takes account of the HRA, RIPA, the Criminal Procedure and Investigations Act 1996 ("CPIA"), GDPR, DPA and the National Police Chiefs' Council Guidance on Open Source Investigation/Research

2.3 This policy and associated procedure will be followed at all times and should be read, where required, alongside the Home Office RIPA Codes of Practice and any other legislation and relevant LDC policies mentioned in this document. Further advice on the interpretation and implementation of this policy should be sought from LDC's RIPA Monitoring Officer, Oliver Dixon.

2.4 Not adhering to this policy could result in the relevant officer(s) being dealt with through the Council's disciplinary procedure.

2.5 This policy is an open document and fully disclosable under the Freedom of Information Act 2000.

## 3. Risk

3.1 Officers should be made aware that any activity carried out over the internet leaves a trace or footprint which can identify the device used, and, in some circumstances, the individual carrying out the activity. Unless the activity is conducted lawfully, LDC may face legal proceedings for breaching the Article 8 right of the person who is the subject of the research or investigation. There are also legal and reputational risks in failing to handle private information in accordance with GDPR and DPA – see further at paragraph 6.

3.2 Due to the potential risk of compromise to other investigations, the activity should be conducted in a manner that does not compromise any current or future investigation or tactics.

## 4. Necessity / Justification

4.1 To justify the research or investigation, there must be a clear lawful reason, and it must be necessary. Therefore the reason for the research, such as the criminal conduct that it is aimed to prevent or detect, must be identified and clearly described. This should be documented with clear objectives. Should the research or investigation fall within the scope of RIPA (i.e. by amounting to 'directed surveillance'[1]), the activity must not proceed without prior

[1] RIPA defines 'directed surveillance' as surveillance that is covert and carried out–
(i) in connection with a specific investigation or operation;

authorisation in accordance with RIPA procedures, including the need to show necessity on specified statutory grounds.

## 5. Proportionality

5.1 Proportionality involves balancing the intrusiveness of the research on the subject and other innocent third parties who might be affected by it (collateral intrusion) against the need for the activity in operational terms. This requires an evaluation of the benefit to carrying out the activity relative to the seriousness of the suspected conduct under research or investigation, and of the expected benefit of the activity versus the privacy intrusion.

5.2 The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

5.3 Where online activity amounts to directed surveillance, part of the application for prior authorisation requires the applicant to demonstrate proportionality to the standard required by RIPA and its relevant Code of Practice.

## 6. Private Information

6.1 RIPA provides that 'private information' includes any information relating to a person's private or family life. Private information should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.

6.2 Prior to, and during any research, staff must take into account the privacy issues regarding any person associated with the research.

## 7. Reviewing the Online Activity

7.1 During the course of conducting the internet open source research or investigation, the nature of the online activity may evolve. Officers involved should continually assess and review their activity to ensure it remains lawful and compliant. Where it starts as or evolves into RIPA activity, the RIPA procedure must be followed. If in doubt, officers should seek advice from the RIPA Monitoring Officer.

(ii) in a manner likely to obtain private information; and
(iii) as a planned response to events or circumstances

## 8. Use of Material

8.1 The material obtained from open source internet and social media research or investigations may be used as intelligence or evidence.

8.2 Any material gathered from the internet during the course of a criminal investigation must be retained in compliance with the CPIA Code of Practice and processed in line with the GDPR.

## 9. Review of Policy

9.1 LDC's Audit and Standards Committee will review this policy annually but may, where justified, resolve to amend it at any time.