Report to:	**Audit and Standards Committee**
Date:	**14 September 2020**
Title:	**Covert Surveillance Policies**
Report of:	**Assistant Director of Legal and Democratic Services**
Ward(s):	**All**
Purpose of report:	**To seek approval of proposed covert surveillance policy changes.**
Officer recommendation(s):	**(1) That the Committee approve–** **a) Lewes and Eastbourne Councils' updated policy on the use of covert surveillance and/or covert human intelligence sources, as set out in Appendix 1; and** **b) The Councils' policy on the acquisition of communications data, as set out in Appendix 2.** **(2) That the Committee grant delegated authority to each of the Chief Finance Officer and the Assistant Director of Legal and Democratic Services to implement the above policies.**
Reasons for recommendations:	**The Committee's role includes oversight of the Lewes District Council's surveillance governance arrangements.**
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 A report setting out the key recommendations of the Investigatory Powers Commissioner's Office (IPCO) inspection of Lewes and Eastbourne Councils carried out in December 2019 was prepared for the Audit and Standards Committee meeting of 17 March 2020. A link to the report is provided as a background paper in paragraph 11 below.

The 17 March meeting had to be cancelled due to the coronavirus pandemic, but the report was for noting only and officers have continued to implement IPCO's recommendations in the meantime.

1.2 The recommendations included the need for (a) certain changes to the Councils' covert surveillance policy; and (b) provision to be made for the lawful acquisition of communications data for investigative purposes.

1.3 Today's report seeks approval of an updated covert surveillance policy and, for the first time, a policy on the acquisition of communications data.

2 Proposed amendments to Covert Surveillance Policy

2.1 IPCO recommended that the Councils' Covert Surveillance Policy provides guidance on the use of a Covert Human Intelligence Source ('CHIS' – see definition in 2.2. below), including arrangements for the appointment of persons fulfilling the role of 'handler' and 'controller' if and when a CHIS is deployed. IPCO further recommended that the policy explains how the role of CHIS differs from a person volunteering information to the Council.

2.2 A CHIS is someone (the source) who establishes a personal relationship with a person (the suspect) for the covert purpose of obtaining intelligence or disclosing information relating to the behaviour of the suspect. The Councils may use a CHIS only for the purpose of preventing or detecting crime or for preventing disorder.

2.3 Accordingly, the amended policy at Appendix 1 of this report sets out the way in which the Councils should manage the deployment of a CHIS (see paragraphs 12-14) and their procedure for reviewing and renewing a CHIS authorisation (see paragraphs 16-18). The distinction between a CHIS and a member of public merely volunteering information to the Council is explained at Appendix 2(b) of the policy.

2.4 In response to a further IPCO recommendation, the amended policy also provides for the processing of confidential information obtained from surveillance (see paragraphs 19-23).

3 Proposed Communications Data Acquisition Policy

3.1 IPCO recommended that Lewes and Eastbourne Councils include in their Covert Surveillance Policy their stance on the use of communications data for investigative purposes, as permitted under the Investigatory Powers Act 2016. Due to the different statutory framework applicable to the two regimes (i.e. the Regulation of Investigatory Powers Act 2000 for directed surveillance and CHIS; and the Investigatory Powers Act 2016 for the acquisition of communications data), officers considered it more appropriate to draw up separate policies.

3.2 Accordingly, the Councils' proposed separate policy on the acquisition of communications data is set out in Appendix 2 of this report. The policy sets out the type of data the Councils may lawfully acquire when seeking to prevent or detect serious crime, and authorisation procedures.

3.3 To date, Lewes and Eastbourne Councils have not needed to use its data communications acquisition powers for investigative purposes. However, it is considered good practice to maintain a policy and procedure for doing so, should the need arise.

4 Alignment of policies

4.1 In keeping with the Councils' approach to corporate policies, the two policies referred to in this report are aligned across Lewes and Eastbourne Councils. This helps to ensure consistent controls and implementation for both locations.

4.2 An equivalent report is to be considered by Eastbourne Borough Council's Audit and Governance Committee on 9 September 2020. Should that Committee approve the two policies but subject to certain amendments, these variations will be put to the Audit and Standards Committee by way of a verbal update. Should the Lewes committee propose any amendments of its own, the report author will consult the Audit and Governance Committee chair as to next steps.

5 Policy Review

5.1 Under the proposed Covert Surveillance Policy, there is no change to the requirement that the Councils' Audit committees receive an annual report on its implementation (see Appendix 1, paragraph 27). Officers will ensure that a suitable report is brought to both committees at the appropriate time each year.

5.2 The proposed policy on data communications acquisition contains an equivalent requirement (see Appendix 2, paragraphs 8.1 to 8.3)

6 Financial appraisal

6.1 The cost of implementing the two policies referred to in this report will be met from existing service budgets.

7 Legal implications

7.1 The Councils are strongly advised to adopt IPCO's recommendations, so as to improve compliance with surveillance legislation and supporting codes of practice. Doing so reduces the Councils' exposure to risk of evidence from surveillance being ruled inadmissible, and the risk of civil claims from individuals in connection with their right to respect for their private and family life.

Lawyer consulted 19.08.20 *Legal ref: 005383-JOINT-OD*

8 Risk management implications

8.1 The Councils' arrangements for the management of covert surveillance, in terms of policies, procedures and designated roles (e.g. RIPA MO and RIPA authorising officers) should ensure that activity is fully compliant with surveillance and human rights legislation. Member oversight is provided in the way mentioned at 5.1 and 5.2 above, enabling a check on officers' use of surveillance powers over the previous year.

9 Equality analysis

9.1 There are no equality issues associated with this report.

10 Appendices

- Appendix 1 – Proposed Policy on the Use of Covert Surveillance and/or Covert Human Intelligence Sources

- Appendix 2 – Proposed Policy on the Acquisition of Communications Data

11 Background papers

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

- Report prepared for Audit and Standards Committee of 17 March 2020 on the inspection of surveillance governance arrangements: https://democracy.lewes-eastbourne.gov.uk/documents/s14060/Inspection%20of%20surveillance%20governance%20arrangements.pdf
- The Regulation of Investigatory Powers Act 2000: http://www.legislation.gov.uk/ukpga/2000/23/contents
- Home Office Code of Practice on Covert Surveillance and Property Interference (August 2018): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf
- Home Office Code of Practice on Covert Human Intelligence Sources (August 2018): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf
- The Investigatory Powers Act 2016: https://www.legislation.gov.uk/ukpga/2016/25/contents
- Communications Data Code of Practice (November 2018): https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/822817/Communications_Data_Code_of_Practice.pdf