

**Report to:** Audit and Governance Committee

**Date:** 24 November 2021

**Title:** Annual report on Covert Surveillance Management

**Report of:** Head of Legal Services

**Ward(s):** All

**Purpose of report:** To update members on activity under the Council's Covert Surveillance Policy

**Officer recommendation(s):** (1) To note the covert surveillance summary for September 2020 to September 2021

(2) To note the Council's actions to address outstanding recommendations from IPCO's inspection in 2019

**Reasons for recommendations:** Best practice requires an annual update to the Committee on Covert Surveillance Policy adherence

**Contact Officer(s):** Name: Lee Ewan  
Post title: Counter-Fraud Investigations Manager and RIPA Monitoring Officer  
E-mail: [lee.ewan@lewes-eastbourne.co.uk](mailto:lee.ewan@lewes-eastbourne.co.uk)  
Telephone number: 01323 415123

---

## **1 Introduction**

1.1 On 9 September 2020, the Audit and Governance Committee approved:

(i) the Council's updated policy on the use of covert surveillance and covert human intelligence sources; and

(ii) the Council's new policy on the acquisition of communications data.

Both policies were drafted to comply with recommendations stemming from IPCO's (Investigatory Powers Commissioner's Office) 2019 inspection of the Council's surveillance arrangements.

1.2 Officers are required to report annually to the Committee on action taken under these policies. Accordingly, the information set out in this report covers the period since September 2020.

1.3 This report also details actions to address any of IPCO's recommendations still outstanding as at September 2020.

## **2 Covert Surveillance Activity**

2.1 Over the period September 2020 to September 2021, no council officer sought authorisation to conduct directed surveillance<sup>1</sup>; to use a covert human intelligence source (CHIS); or to acquire communications data. Accordingly, no authorisations for these activities were granted during this time.

2.2 The council's Neighbourhood First officers wear highly visible uniforms which helps deter criminal activity in the community. Any surveillance they undertake to deter fly tipping is done using cameras mounted on lamp posts but with highly visible signage intended to make potential offenders aware. Such activity amounts to overt surveillance which falls outside of the scope of this report, as it is not regulated by RIPA 2000 or the Investigatory Powers Act 2016.

## **3 Covert Surveillance and CHIS Readiness**

3.1 IPCO expects district councils to be ready and capable of conducting covert surveillance, even if operations requiring its use are infrequent.

3.2 To ensure continuing capability over the last 12 months, Oliver Dixon, as Senior Responsible Officer for surveillance matters, appointed Linda Farley as a RIPA Authorising Officer to replace former AO, Peter Finnis, who left the Council in late 2020. Linda undertook the necessary training to be able to perform this role when called upon. Tim Whelan remains the Council's other qualified RIPA Authorising Officer.

3.3 In addition, three members of the Council's Counter-Fraud Team received RIPA refresher training earlier this year.

3.4 Despite the Council never having identified the need to use a CHIS, IPCO considered it important for relevant officers to understand the regulatory framework for CHIS deployment and the steps involved in authorising and then managing CHIS operations. To meet this expectation, the RIPA Monitoring Officer has arranged CHIS introductory training with a specialist provider for 16 November 2021. Relevant members of the Legal and Counter-Fraud teams will attend.

## **4 Online Surveillance**

4.1 Certain council teams may from time to time use open source material available on the internet to confirm the identity and circumstances of persons who (a) are in significant debt to the Council and need to be traced or (b) may be the subject of, or associated with, a counter-fraud investigation.

---

<sup>1</sup> Surveillance is "directed" if it is: covert (but not intrusive); conducted for the purposes of a specific operation or investigation; conducted otherwise than in response to immediate events or circumstances; and likely to result in obtaining personal information about a person.

- 4.2 Controls are in place to minimise the risk that use of open source material to confirm an online presence (which, because it is in the public domain, does not intrude on the person's right to a private and family life) does not develop into 'directed surveillance' and therefore require express authorisation to render it a lawful interference with their right to privacy.
- 4.3 Typically, online research may amount to directed surveillance if it becomes highly targeted through focused and systematic monitoring of an individual over a period of time, resulting in a profile or record of that person's activities being created and used, with a view to potential legal proceedings. Such surveillance may lawfully proceed only if it (a) meets the crime threshold – see paragraph 4.5 below; and (b) is authorised in accordance with RIPA procedures.
- 4.4 Controls are also in place to ensure that creating a covert profile to establish an online connection with a person whose social media profile is not open to the public may not proceed without the necessary authorisation.

The RIPA Monitoring Officer is meeting with the relevant Council teams to review the control arrangements and reinforce compliance.

- 4.5 The Council must not authorise directed surveillance unless the activity under investigation reaches the crime threshold, namely a criminal offence that is punishable, whether on summary conviction or indictment, by a maximum term of at least 6 months' imprisonment. Historically, the directed surveillance operations conducted by the Council have all related to fraud within the ambit of the Fraud Act 2006 and therefore liable to a penalty that would meet the crime threshold.

## **5 IPCO Recommendations**

- 5.1 All of IPCO's recommendations made following their inspection of the Council's surveillance management systems in 2019 have now been implemented. Full details are given in the table in Appendix 1.

## **6 Financial appraisal**

- 6.1 The only expenditure associated with IPCO's recommendations is the cost of CHIS training. This will be met from the training budgets of those teams nominating officers for the webinar on 16 November.

## **7 Legal implications**

- 7.1 For the Council's directed surveillance, use of a CHIS or acquisition of communications data to be compatible with Human Rights legislation and therefore lawful, it must comply with the controls and procedures set down by the Regulation of Investigatory Powers Act 2000 or the Investigatory Powers Act 2016 (as applicable). The Council must also have regard to the relevant Home Office codes of practice which set out the practical steps local authorities should follow in applying these regulatory controls.

## **8 Risk management implications**

- 8.1 Failure to implement IPCO's recommendations brings with it the risk of (1) non-compliance with surveillance legislation and codes of practice; and (2) censure by IPCO at their next inspection, due in December 2022, causing reputational harm to the Council.

## **9 Equality analysis**

There are no equality issues associated with this report.

## **10 Appendices**

- Appendix 1 – IPCO recommendations and the Council's response

## **11 Background papers**

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

- Covert surveillance report to Audit and Governance Committee, dated 9 September 2020. <https://democracy.lewes-eastbourne.gov.uk/documents/s17820/Covert%20Surveillance%20Policies%20Report%20to%20Audit%20Governance%20Ctee%20August%202020.pdf>