

<b>Report to:</b>	<b>Audit and Governance Committee</b>
<b>Date:</b>	<b>10 December 2024</b>
<b>Title:</b>	<b>Annual report on Covert Surveillance Management</b>
<b>Report of:</b>	<b>RIPA (Regulation of Investigatory Powers Act) Monitoring Officer</b>
<b>Ward(s):</b>	<b>All</b>
<b>Purpose of report:</b>	<b>To provide an overview of the Council’s use of covert surveillance and acquisition of communication data powers in 23/24.</b>
<b>Officer recommendation(s):</b>	<b>To note the covert surveillance summary for September 2023 to September 2024.</b>
<b>Reasons for recommendations:</b>	<b>Best practice requires an annual update to the Committee on Covert Surveillance Policy adherence.</b>
<b>Contact Officer(s):</b>	<b>Name: Lee Ewan Post title: Counter-Fraud Investigations Manager and RIPA Monitoring Officer E-mail: <a href="mailto:lee.ewan@lewes-eastbourne.gov.uk">lee.ewan@lewes-eastbourne.gov.uk</a> Telephone number: 01323 415123</b>

---

## **1 Introduction**

- 1.1 This report summarises the Council’s use of covert surveillance powers and acquisition of communication data gathered from September 2023 to September 2024.
- 1.2 It also highlights the governance arrangements and preparation for the Investigatory Powers Commissioner’s Office (IPCO) inspection anticipated to take place in June 2025.

## **2 Directed Surveillance Legislative and Policy Background**

- 2.1 Part 2 of the Regulation of Investigatory Powers Act 2000 (‘RIPA’) provides for the authorisation by certain public bodies, including Lewes District Council, of ‘Directed Surveillance’.
- 2.2 ‘Directed Surveillance’ is covert surveillance carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private information about any person, other than by way of immediate response to events or circumstances.

- 2.3 In conducting directed surveillance, the Council must comply not just with RIPA but with the relevant Home Office code of practice and the Council's own policy, links to which are provided in paragraph 10 below.
- 2.4 In procedural terms, the most important steps under RIPA are for the directed surveillance to be authorised internally by a trained and designated senior manager, and for that authorisation to be approved by a justice of the peace, i.e. a magistrate or district judge.
- 2.5 At both stages, the authorising officer and JP must be satisfied that the proposed surveillance is necessary for the prevention or detection of a crime punishable, on conviction, by a custodial sentence of at least six months; and is proportionate to what is sought to be achieved by carrying it out. This involves balancing the seriousness of the intrusion into the privacy of the subject (or any other person who may be affected) against the need for the activity in investigative and operational terms.

### **3 Governance Arrangements**

- 3.1 IPCO provides independent oversight of the use of investigatory powers by intelligence agencies, police forces and other public authorities. Its purpose is to oversee how these powers are used, taking account of the public interest and ensuring that investigations are conducted in accordance with the law.
- 3.2 IPCO's oversight includes the inspection of the public authorities. Lewes and Eastbourne Councils are inspected once every three years, most recently in June 2022. Details of this inspection and recommendations were presented and noted by the Audit and Governance Committee in the annual surveillance management report on 13 November 2023.
- 3.3 Internally, the Council regulates its use of surveillance powers through specially trained managers, consisting of:
- RIPA Senior Responsible Officer – Oliver Dixon
  - RIPA Monitoring Officer – Lee Ewan
  - RIPA Authorising Officers – Linda Farley and one additional vacancy – an appointment will be made by CMT shortly
- 3.4 To ensure continuing capability over the past 12 months, Linda Farley attended a RIPA Authorising Officer refresher course in February 2024. Three Counter-Fraud Investigation Officers attended a RIPA refresher course in May 2024. Training and system access was also organised in May 2024 for Linda Farley and officers within the Counter-Fraud team to access Communications Data; further information can be found in paragraph 5 below.
- 3.5 Training for the current vacant RIPA Authorising Officer will be organised upon the next available opportunity once this position has been filled. Oliver Dixon and Lee Ewan will also be due to attend respective refresher courses in their roles as RIPA Senior Responsible Officer and RIPA Monitoring Officer within the next 12 months to maintain up to date knowledge and capability.

3.6 Surveillance arrangements are also subject to periodic internal audit.

#### **4 Use of Covert Surveillance Powers between September 2023 and September 2024**

4.1 Over the period September 2023 – September 2024, no council officer sought authorisation to conduct directed surveillance or to use a covert human intelligence source (CHIS). Accordingly, no authorisations for these activities were granted during this time.

4.2 The non-use of directed surveillance powers is in part explained by the strict criteria relating to authorisation, as detailed in Paragraph 2.5 above. The Council continues to investigate suspected criminal offences (mainly fraud), breach of tenancy agreements and non-payment of fees or taxes but, in the majority of cases, directed surveillance cannot be justified under RIPA criteria and is therefore not used.

#### **5 Acquisition of Communications Data and use of these powers between September 2023 and September 2024**

5.1 Part 3 of the Investigatory Powers Act 2016 (“the Act”) permits certain public bodies to acquire specified types of communications data in limited circumstances, subject to prior authorisation granted in accordance with the Act. The Act grants powers to local authorities to acquire data in relation to cases involving the prevention or detection of serious crime.

5.2 The communications data which, in defined circumstances, local authorities are permitted to obtain under the Act is known as ‘entity data’ and ‘events data’. This broadly contains data which can identify who a suspected offender has been in communication with, or their location via the movement of their mobile phone. However, the Act does not permit the Council to monitor the content of the call.

5.3 The application process for obtaining Communications Data is centralised through the National Anti-Fraud Network (NAFN) who act as a single point of contact for local authorities. Where an application meets the threshold requirements, internal authorisation is still required by one of the council’s Authorising Officers before NAFN review the application and liaise with communication providers to obtain the entity and/or events data.

5.4 Lewes District Council had previously not sought to obtain Communications Data or had access to the NAFN application system. In May 2024 training and access to the application system was provided by NAFN to the council’s Authorising Officer, RIPA Monitoring Officer and Counter-Fraud Investigation officers.

5.5 Following the implementation of access to the NAFN system, two applications for Communications data have been made and authorised which covers the period up until September 2024.

## **6 IPCO inspection**

6.1 IPCO made one recommendation following their inspection of the Council's surveillance management systems in June 2022, which has been implemented. The recommendation centred on amendments to the Council's RIPA policies to incorporate the retention, review and destruction (RRD) of data gathered utilising the covert powers available. On 14 November 2022, the Audit and Standards 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.

6.2 In accordance with the updated policies (see paragraph 10, background papers) a new recording process has been introduced to incorporate Communications Data, which will provide compliance with the RRD requirements and held for future inspection by IPCO. An existing RRD process is held for directed surveillance cases, however no applications have been made since the last IPCO inspection.

6.3 It is anticipated the Council's next inspection by IPCO will be due in June 2025, and work has already begun in preparation for this inspection.

## **7 Financial appraisal**

7.1 There are no immediate financial implications associated with this report, however the committee should note that there is a small cost associated with the training costs for three officers estimated to be £1,000.

*Date of financial input: 11.11.24*

## **8 Legal implications**

8.1 For the Council's directed surveillance, use of a CHIS or acquisition of communications data to comply with human rights legislation (specifically the right to respect for family and private life, and the right to a fair trial), 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.

*Date of legal input: 16.10.24*

*Legal ref: 11448-JOINT-OD*

## **9 Risk management implications**

9.1 Failure to implement IPCO's recommendations brings with it the risk of (1) non-compliance with surveillance legislation and codes of practice, leading to a potential challenge by affected parties that could undermine the validity of data

collected; and (2) censure by IPCO at their next inspection, causing reputational harm to the Council.

## **10 Background papers**

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

- [Home Office Code of Practice on Covert Surveillance and Property Interference \(August 2018\)](#)
- [Home Office Code of Practice on Communications Data \(November 2018\)](#)
- [LEC's policy on use of covert surveillance and/or covert human intelligence sources](#)
- [LEC's policy on the acquisition of communications data](#)