Agenda Item 9

Leicestershire County Council

CORPORATE GOVERNANCE COMMITTEE – 26 JANUARY 2024

REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE INVESTIGATORY POWERS ACT 2016

REPORT OF THE DIRECTOR OF LAW AND GOVERNANCE

Purpose of Report

1. The purpose of this report is:

   (a) to advise the Committee on the Authority's use of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) for the period from 1 January 2023 to 31 December 2023; and

   (b) to ask the Committee to review the Covert Surveillance and the Acquisition of Communications Data Policy Statement relating to RIPA which is attached to this report.

Policy Framework and Previous Decisions

2. The Codes of Practice made under RIPA require elected members of a local authority to review the authority's use of RIPA and the policy at least once a year. The Corporate Governance Committee as the relevant committee for this purpose is also required to consider internal reports on the use of surveillance to ensure that it is being applied consistently with the local authority's policy and that the policy remains fit for purpose. The Code makes it clear that elected members should not be involved in making decisions on specific authorisations.

3. On 27 January 2023 this Committee agreed that the Council's Covert Surveillance and the Acquisition of Communications Data Policy Statement (relating to the use of RIPA) remained fit for purpose. As there are no proposed changes to the Policy Statement again this year there is no requirement for further review by the Cabinet.

Background

4. RIPA provides a framework to ensure investigatory techniques are used in a way that is compatible with Article 8 (right to respect for private and family life) of the European Convention on Human Rights (ECHR). RIPA ensures that

these techniques are used in a regulated way and it includes safeguards to prevent abuse of such methods. Use of these covert techniques will only be authorised if considered lawful, necessary and proportionate.

5. The Trading Standards Service is the primary user of RIPA and IPA within the County Council and it mainly undertakes the following three activities:

   i. Directed Surveillance (DS)– the pre-planned covert surveillance of individuals, sometimes involving the use of hidden visual and audio equipment.
   ii. Covert Human Intelligence Sources (CHIS) – the use of County Council officers, who act as consumers to purchase goods and services, e.g. in person, by telephone or via the internet.
   iii. Communications data (CD) – the acquisition of communications data, for example, subscriber details relating to an internet account, a mobile phone or fixed line numbers, but such data does not include the contents of the communication itself.

6. The Investigatory Powers Commissioner's Office (IPCO) oversee the use of covert investigatory powers by more than 600 public authorities, including the UK's intelligence agencies, law enforcement agencies, police, councils and prisons.

7. Employees of the council should not engage in or commission any form of surveillance without first contacting one of the County Council RIPA authorising officers. If a DS or CHIS is in principle approved internally the application must then be submitted to the Magistrates' Court for the final authorisation.

8. The Director of Law and Governance is the designated Senior Responsible Officer for ensuring that all authorising officers (currently the Council's Head of Regulatory Services and Assistant Head of Law) suitably qualified and experienced to undertake the role and that the County Council RIPA policy and operational procedures remain fit for purpose

Communications Data

9. The Data Retention and Acquisition Regulations (SI 2018/1123) provide an authorisation process for public bodies that seek to obtain communications data for a specific criminal investigation.

10. Judicial oversight of local authorities seeking to covertly obtain communications is administered by the Office of Communications Data Authorisations (OCDA).

11. The legislation requires local authorities to enter into a formal collaboration agreement with the National Anti-Fraud Network (NAFN) an organisation, hosted by Tameside Metropolitan Borough Council which specialises in providing data and intelligence services to enforcement agencies. NAFN act as the single point of contact between any communications service provider

and the Council and prepare, on the Council's behalf, any applications to the OCDA.

12. An application to obtain communications data must first receive senior internal approval by the designated person (currently the Council's Head of Regulatory Services and Assistant Head of Law) before it can be submitted to the OCDA for consideration. An application will therefore only be referred to the OCDA if it first meets the Council's own necessity and proportionality test.

13. Local authorities will be permitted via NAFN to acquire the less intrusive types of communications data, now referred to as '*entity' data* (e.g., the identity of the person to whom services are provided) and '*events' data* (e.g. the date and type of communications, time sent, and duration, frequency of communications). However, it will remain the case that under no circumstances will it be permitted to obtain or intercept the content of any communications.

14. In order to obtain either type of data, in addition to satisfying the necessity and proportionality test, an authority must show that the purpose of the application is for the prevention and detection of a crime. For *'events'* data, the threshold is raised and the purpose must be for the prevention or detection of a *'serious'* crime (e.g. an offence for which an individual could be sentenced to imprisonment for a term of 12 months or more, or offences which involve, as an integral part, the sending of a communication or a breach of a person's privacy).

15. Any application to the OCDA will be guided by the Council's Policy Statement attached, current best practice and the Communications Data Code.

Surveillance activities

16. For the period 1 January – 31 December 2023, the following authorisations were approved:

- 1 relating to cover human intelligence sources (CHIS)
- 1 relating to Directed Surveillance (DS)
- 8 applications to obtain communications data.

17. All authorisations were granted by the Court following the Council's internal approval process referred to above and all were associated with criminal investigations undertaken by the Trading Standards Service.

18. The County Council's Intranet continues to be the primary source of information and advice to ensure all County Council managers are aware of the authorisation, necessity and proportionality requirements when considering deployment of covert surveillance. The Policy Statement also references the requirement for managers to liaise with an authorising officer before deploying any form of covert activity, which may include systematically accessing open-source material including social media material.

Recommendations

19. The Committee is asked to:

a) note the use of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) for the period from 1 January to 31 December 2023;

b) review the Council's Covert Surveillance and the Acquisition of Communications Data Policy Statement (which is unchanged since approval by Cabinet in March 2021) and confirm that this remains fit for purpose;

c) agree to continue to receive an annual report on the use of RIPA and IPA powers.

Background Papers

Report to the Corporate Governance Committee on 27 January 2023 - Regulation of Investigatory powers Act 2000 and the Investigatory Powers Act 2016
https://democracy.leics.gov.uk/ieListDocuments.aspx?CId=434&MId=7128&Ver=4

Report to the Cabinet on 23 March 2021 Regulation of Investigatory powers Act 2000 and the Investigatory Powers Act 2016 - Review of Policy statement
https://democracy.leics.gov.uk/ieListDocuments.aspx?CId=135&MId=6441&Ver=4

Circulation under the Local Issues Alert Procedure

None.

Equality Implications

None arising from this report.

Human Rights Implications

None.

Officer to Contact

Lauren Haslam
Director of Law and Governance
Tel: 0116 305 6240
Email: lauren.haslam@leics.gov.uk

Appendices

Appendix - Covert Surveillance and the Acquisition of Communications Data Policy Statement.