Agenda Item 15

Leicestershire County Council

CABINET – 23 MARCH 2021

REGULATION OF INVESTIGATORY POWERS ACT 2000 AND THE INVESTIGATORY POWERS ACT 2016 - REVIEW OF POLICY STATEMENT

REPORT OF THE DIRECTOR OF LAW AND GOVERNANCE

PART A

Purpose of the Report

1. The purpose of this report is to advise the Cabinet on the Council's use of the Regulation of Investigatory Powers Act 2000 (RIPA) and the Investigatory Powers Act 2016 (IPA) for the period from 1 October 2019 to 31 December 2020 and the fact that there have been no changes to legislation relating to the acquisition of communications data by local authorities. In light of this, this report also seeks agreement that the existing Policy Statement remains fit for purpose.

Recommendations

2. It is recommended that:

   (a) The Council's use of the Regulation of Investigatory Powers Act 2000 (RIPA) for the period 1 October 2019 to 31 December 2020 be noted;

   (b) The Council's existing Covert Surveillance and the Acquisition of Communications Data Policy Statement on the use of RIPA powers (appended to this report) is agreed as fit for purpose.

Reasons for Recommendations

3. The Codes of Practice made under RIPA require elected members of a local authority to review the Authority's use of RIPA and to set the Policy at least once a year. They should also 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. Elected members should not, however, be involved in making decisions on specific authorisations.

4. The Council's current Policy Statement was approved by the Cabinet on 24 May 2019. There have been no legislative changes since that date, therefore the Policy Statement remains fit for purpose.

Timetable for Decisions (including Scrutiny)

5. The Corporate Governance Committee considered a report on the Regulation of Investigatory Powers Act 2000 and Investigatory Powers Act 2016 at its meeting on 29 January 2021 and agreed to recommend to the Cabinet that the current Covert Surveillance and the Acquisition of "Communications Data" Policy Statement on the use of RIPA remained fit for purpose.

Policy Framework and Previous Decisions

6. On 10 May 2019, the Corporate Governance Committee considered proposed changes to the Council's RIPA Policy Statement made to reflect legislative changes and best practice. The Cabinet subsequently approved the revised Policy Statement at its meeting on 24 May 2019.

7. On 29 January 2021, the Corporate Governance Committee reviewed the existing Policy Statement and agreed to recommend to the Cabinet that it remained fit for purpose.

Resources Implications

8. There are no resources implications arising from this report.

Circulation under the Local Issues Alert Procedure

9. None.

Officers to Contact

Lauren Haslam, Director of Law and Governance
Tel: 0116 305 6007
Email: Lauren.Haslam@leics.gov.uk

Gary Connors, Head of Regulatory Services, Chief Executives Department
Tel: 0116 305 6536
Email: gary.connors@leics.gov.uk

PART B

Background

10. RIPA provides a framework to ensure investigatory and surveillance 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. 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 legal, necessary and proportionate.

11. 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 – the pre-planned covert surveillance of individuals, sometimes involving the use of hidden visual and audio equipment.

    ii. Covert Human Intelligence Sources – 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 – the acquisition of communications data, for example, subscriber details relating to an internet account, a mobile phone or fixed line numbers, but not the contents of the communication itself.

12. In September 2017 the Investigatory Powers Commissioner's Office (IPCO) took over responsibility for oversight of investigatory powers from the Interception of Communications Commissioner's Office (IOCCO), the Office of Surveillance Commissioners SC and the Intelligence Services Commissioner (ISComm). IPCO is now responsible for the audit functions of these former bodies and has oversight of Office of Communications Data Authorisations as detailed below.

13. The Codes of Practice made under RIPA require elected members of a local authority to review the Authority's use of RIPA and to set the Policy at least once a year. The timing of this review has been delayed due to the Covid-19 pandemic.

14. The Covert Surveillance and the Acquisition of Communications Data Policy Statement was approved by the Cabinet on 24 May 2019. There have been no changes to the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016 since that date, so the Council's current Policy Statement remains fit for purpose.

Surveillance Activities

15. Activities under Direct Surveillance and Covert Human Intelligence Sources must be authorised by the Magistrates' Court.

16. For the period of 1 October 2019 –31 December 2020 the following authorisations were approved:

    - Three relating to Covert Human Intelligence Sources (CHIS)

    - Three applications to obtain communications data.

17. All authorisations granted within this period were associated with criminal investigations undertaken by the Trading Standards Service.

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

Communications Data

19. The Data Retention and Acquisition Regulations (SI 2018/1123) amended both the Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016 (IPA) and provided an authorisation process for public bodies that seek to obtain communications data for a specific criminal investigation.

20. Judicial oversight of local authorities seeking covertly to obtain communications transferred from the Magistrates' Court to the Office of Communications Data Authorisations (OCDA).

21. 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.

22. An application to obtain communications data must first receive senior internal approval by the designated person 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.

23. Local authorities will be permitted 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.

24. To obtain either type of data, in addition to satisfying the necessity and proportionality test, an authority previously had to show that the purpose for the application was for the prevention and detection of a crime. This remains the

same for *'entity'* data. However, for *'events'* data, the threshold has been raised and the purpose must now be for the prevention or detection of a *'serious'* crime. This is 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.

25. Any application to the OCDA will be guided by the Council's Policy Statement, appended to this report, current best practice and the Communications Data Code.

Equality and Human Rights Implications

26. There are no Equality and Human Rights Implications arising from this report.

Background Papers

Report to the Cabinet 24 May 2019 - Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016 - Review of Policy Statement
http://politics.leics.gov.uk/ieListDocuments.aspx?CId=135&MId=5603&Ver=4

Report to the Corporate Governance Committee 29 January 2021 - Regulation of Investigatory Powers Act 2000 and the Investigatory Powers Act 2016.
http://politics.leics.gov.uk/ieListDocuments.aspx?CId=434&MId=6492&Ver=4

Appendix

Covert Surveillance and the Acquisition of Communications Data Policy Statement.

This page is intentionally left blank