Leicestershire County Council

CORPORATE GOVERNANCE COMMITTEE – 29 JANUARY 2021

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 to:

   (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 October 2019 to 31 December 2020; 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 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.

3. On 10 May 2019 this Committee agreed changes to the Council's RIPA Policy Statement to reflect legislative changes and best practice. The Cabinet subsequently approved the revised Policy Statement at its meeting on 24 May 2019

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 legal, 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 – the pre-panned 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 such data does not include the contents of the communication itself.

6. 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 are now responsible for the audit functions of these former bodies and have oversight of Office of Communications Data Authorisations as detailed below.

Communications Data

7. 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.

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

9. 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.

10. An application to obtain communications data must first receive senior internal approval by the delegated 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.

11. 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.

12. In order to obtain either type of data, in addition to satisfying the necessity and proportionality test, an authority previously had to show 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 (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).

13. 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

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

- Three relating to cover human intelligence sources (CHIS)
- Three applications to obtain communications data.

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

16. 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 material social media material.

Recommendations

17. The Committee is asked to:

i. notes the report 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 October 2019 to 31 December 2020; and

ii. recommend to Cabinet that the County Council's Policy Statement on the use of RIPA powers remains fit for purpose.

iii. agree to continue to receive an annual report on the use of RIPA powers and to report to the Cabinet on an annual basis on both the use of RIPA powers and whether the Policy remains fit for purpose.

Background Papers

Report to the Corporate Governance Committee on 10 May 2019
http://politics.leics.gov.uk/ieListDocuments.aspx?CId=434&MId=5854&Ver=4

Report to the Cabinet on 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

Circulation under the Local Issues Alert Procedure

None.

Equality and Human Rights Implications

None arising from this report.

Officers 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 .