

Meeting Audit Committee
Portfolio Area Information Governance – ICT Services
Date 8 November 2023



REGULATION OF INVESTIGATORY POWERS ACT (RIPA) POLICY

NON-KEY DECISION

1 **PURPOSE**

- 1.1 To present the Council’s updated Regulation of Investigatory Powers Act (RIPA) Policy for consideration by the Committee, to ensure the Council as a public authority meets its obligations under the Regulation of Investigatory Powers Act 2000.

2 **RECOMMENDATIONS**

- 2.1. That the content of the report be noted.
- 2.2. That the updated Regulation of Investigatory Powers Act (RIPA) Policy, as attached at Appendix A to the report, be approved.

3 **BACKGROUND**

- 3.1 RIPA regulates the use of certain surveillance powers by public authorities, including:

- Directed Surveillance (covert surveillance conducted as part of a specific investigation likely to result in obtaining private information about an individual)
- Use of Covert Human Intelligence Sources (CHIS), and
- Access to communications data (e.g. details of subscribers to telephone numbers or email accounts).

- 3.2 The Council is a rare user of these powers. However, it is important that it has sufficient oversight of its activities to ensure that any considered use is compliant with individuals' human rights and compliance with legislative provisions.
- 3.3 The Home Office publishes national Codes of Practice on the use of RIPA powers by public authorities. These help public authorities assess and understand whether and in what circumstances it is appropriate to use covert techniques. The codes also provide guidance on what procedures need to be followed in each case. The Council must have regard to the relevant Code of Practice whenever exercising powers covered by RIPA. The Investigatory Powers Commissioner (IPC) conducts regular inspections of all public authorities to ensure compliance with RIPA, and the Codes of Practice.
- 3.4 External Inspections are carried out from time-to-time by the Investigatory Powers Commissioner's Office ('IPCO'), so it is important that all documentation is properly completed and (where relevant) authorised to confirm that any directed surveillance is carried out on a lawful basis. The last inspection was held in July 2023. The Council will be due for a further review on or around 2026 dependent on the IPCO's inspection scheduling requirements.
- 3.5 The Council is required to have arrangements and a RIPA Policy in place. The current one was approved in 2017/18.
- 3.6 Members should note the Council last used its surveillance powers in 2021.
- 3.7 The Shared Anti-Fraud Service ('SAFs') that the Council is a member of, also utilise such powers and these are regulated through Hertfordshire County Council's processes.
- 3.8 In terms of Communications data, all such applications must be processed through the Nafn (National Anti-Fraud Network), who will consider the application prior to submitting this for approval to the Office for Communications Data Authorisations (OCDA). All applications must be approved before Communications Data is acquired. All applications submitted to NAFN will be overseen by the Council's Borough Solicitor who acts as the Council's single point of contact for such applications. This means there is an experienced person that ensures controls and checks on any applications that are considered by Stevenage Borough Council.
- 3.9 RIPA training has been provided to Council authorising officers in 2021 and further officer training is in the process of being arranged for 2023/24.

4 REASONS FOR RECOMMENDED COURSE OF ACTION AND OTHER OPTIONS

- 4.1 From the Council's recent inspection, it was recommended the Council raise awareness of its RIPA Policy amongst officers and elected members, to increase understanding of RIPA arrangements in the Council.
- 4.2 To help improve understanding of the procedures for directed surveillance applications, the Policy has been reviewed and updated with a revised RIPA management structure that identifies the Council's senior authorising officers involved in the application process and inclusion of a RIPA Process Flow Chart and Social Media Evidence Log Template located under Appendix A of the Policy.
- 4.3 Further powers have been granted to public authorities under Sections 37 to 44 of the Police, Crime, Sentencing and Courts Act 2022 that came into force on 8 November 2022. This provides public authorities with a further power to extract Communications Data held on electronic devices. Such legislative changes makes it more important for the Council to have a Policy in place that ensures proper procedure is followed.

5 IMPLICATIONS

Financial Implications

- 5.1 There are no financial implications arising from this Report.

Legal Implications

- 5.2 The Regulation of Investigatory Powers Act 2000 ("RIPA") enables local authorities to carry out certain types of surveillance activity, as long as specified procedures are followed. The information obtained as a result of surveillance operations can be relied upon in court proceedings providing RIPA is complied with.
- 5.3 Full details of the RIPA requirements and compliance are set out in the Policy, with relevant documents and guidance document available to relevant officers via the staff intranet should they consider it necessary to use these powers.

Equalities and Diversity Implications

- 5.4 In line with the Public Sector Equality Duty, public bodies must, in the exercise of their functions, give due regard to the need to eliminate discrimination, harassment, victimisation, to advance equality of opportunity and foster good relations between those who share a protected characteristic and those who do not.
- 5.5 The contents of this report do not directly impact on equality, in that it is not making proposals that will have a direct impact on equality of access or outcomes for diverse groups.

BACKGROUND DOCUMENTS

BD1 [CHIS Code \(publishing.service.gov.uk\)](https://publishing.service.gov.uk)

BD2 [Extraction of Information from electronic devices: code of practice \(publishing.service.gov.uk\)](https://publishing.service.gov.uk)

APPENDICES

A RIPA Policy