Member Report - For Information

RIPA Monitoring Report for 2023/24

Public

To:	Governance Committee	**Date:**	25 November 2024
From:	Managing Director (Head of Paid Services)	**Decision type:**	For Information
Portfolio:	Resources	**Forward Plan Reference:**	
Priority:	A Strong and Sustainable Council		

---

1. Summary of report

1.1. The report is to provide Members with detail in relation to applications made during the 2023/24 financial year under the Regulation of Investigatory Powers Act 2000 (RIPA), with previous year's comparative data.

2. What are the objectives of the report and how do they link to the Council's priorities?

2.1. The report provides Members with some analysis of the RIPA applications received during the last financial year in order that they can have oversight of the use of RIPA powers within the authority. This will give Member's confidence that RIPA powers are being used proportionately.

2.2. The detailed monitoring of the use of our powers under RIPA is a legal requirement.

3. Background and detail

3.1 The Regulation of Investigatory Powers Act 2000 (RIPA) is a law covering and regulating surveillance. Insofar as local authorities are concerned, amongst other things, it provides statutory safeguards to ensure that when directed surveillance is undertaken, or when communications data is accessed, the use is always fully recorded and transparent.

3.2 Local Authorities have powers under RIPA to undertake directed surveillance and to acquire communications data as part of their investigations. "Directed surveillance" involves using covert methods of surveillance where there is a likelihood of private information being obtained. In such circumstances, the operation needs to be authorised. It should be noted that local authorities have no power to grant authorisations for intrusive surveillance and should only undertake operations for the purpose of preventing or detecting crime. "Intrusive surveillance" is where, for example, surveillance is taking place within residential premises or in a private vehicle.

3.3. If surveillance is planned and falls into a category covered by RIPA, authorisation must be obtained. The Protection of Freedoms Act 2012 requires local authorities to obtain the approval of a Magistrate for the use of Directed Surveillance or the deployment of a Covert Human Intelligence Source (CHIS). An approval is also required if an authorisation to use such techniques is being renewed.

3.4. In each case, the role of the Magistrate is to ensure that the correct procedures have been followed and the relevant factors have been taken account of. The provisions allow the Magistrate, on refusing an approval of an authorisation, to quash that authorisation.

3.5. A local authority can only authorise Directed Surveillance in cases where the offence under investigation carries a potential custodial sentence of six months or more (the Serious Crime Test).

3.6. Every application for the use of these powers must consider in detail the necessity of using the powers and the proportionality of such use. Careful consideration to any potential "collateral intrusion" (that is, where the details of or relating to an innocent third party might become known) must be given.

3.7. Enforcement activities undertaken by the authority which fall within the remit of the Regulation of Investigatory Powers Act 2000 are subject to monitoring and oversight by the Investigatory Powers Commissioner's Office.

3.8. A record of all authorisations and associated paperwork must be kept within a central record. This record is subject to quarterly auditing by the Authorising Officer and following each audit a briefing note is provided for the Portfolio Holder for Corporate Resources. The Authorising Officer also has a quarterly meeting with the Senior Officer with overall responsibility for RIPA matters who is the Managing Director (Head of Paid Service).

RIPA authorisations in 2023-24

3.9. During the period 1/4/2023 to 31/03/2024, 1 authorisation to conduct directed surveillance was made by Council Officers. This application was from the Trading Standards section and received Magistrate's approval following authorisation

3.10. The operation related to an investigation into the illegal sale of counterfeit goods via social media. Trading in counterfeit goods is an offence under the Trademarks Act 1994 which carries a maximum penalty of 10 years' imprisonment.

3.11. A linked application for the use of a Covert Human Intelligence Source (CHIS) was also made during this twelve-month period. This was to enable an Officer to engage with the seller in order to secure a test purchase.

3.12. There were no applications which required the use of urgency provisions. At the end of this financial year, no Directed Surveillance or CHIS applications remained extant.

3.13. The Authority's compliance with RIPA legislation is reviewed approximately every 3 years and as the last inspection was in 2021 an inspector from the Investigatory Powers Commissioner's Office attended on 23 September 2024 to review our compliance with RIPA Legislation. He met with all Officers involved and advised that he would write to us with his findings and feedback. We have yet to receive any response following the inspection.

RIPA Comparative Data from previous years

3.14. The following table indicates the number and type of applications received for the use of directed surveillance and the use of a CHIS, in order to provide a comparison:

Year	Council applications for directed surveillance	Third Party Authorisations	CHIS
2023	1 from Trading Standards	0	1 from Trading Standards
2022	1 from Trading Standards	0	1 from Trading Standards
2021	0	0	0
2020	4 from Trading Standards	0	4 from Trading Standards
2019	4 from Trading Standards	0	4 from Trading Standards
2018	2 from Trading Standards	0	0
2017	2 from Trading Standards	0	2 from Trading Standards
2016	7 from Trading Standards	0	3 from Trading Standards

Communications Data

3.15. The Council uses the National Anti-Fraud Network (NAFN) Membership Agreement in order to obtain Communications Data when it is required in relation to an investigation. This is a support, liaison and advice service which ensures correct authorisation procedures are followed for the acquisition of such data.

3.16. NAFN ensures accredited Single Point of Contact Officers (SPOC's) check all applications for compliance. They support the Designated Persons from the Authority (the Governance Director and Commercial & Legal Manager) who have oversight of applications. Communications Data applications are no longer determined by a Magistrate but by the Office for Communications Data Authorisations (OCDA) which reviews communication data applications independently.

3.17. During 1 April 2023 to 31 March 2024 there were no Communications Data applications submitted. The table below shows the activity where subscriber information was obtained for the purpose of the prevention and detection of crime in previous years.

Year	Number of applications	Reason
2023	0	

2022	1	Trading Standards Operation
2021	1	Trading Standards Operation
2020	4	3 Scambuster Operations 1 Trading Standards Operations
2019	0	
2018	4	3 Scambuster Operations 1 Trading standards Operation
2017	0	
2016	1	Scambuster Trading Standards Operation

4. Appendices and background papers

4.1. No background papers were used in writing this report. The full report from the last inspection dated 15 February 2021 is held on the central records and is available for Members to look at, as will any report from the inspection in September 2024 once this is received.

5. Contact officer

5.1. Name: Christopher Stannard

Position: Principal Legal Officer
Address: Redcar & Cleveland House
Telephone: 01642 444537
Email: Christopher.stannard@redcar-cleveland.gov.uk