For Publication

Regulation of Investigatory Powers Act 2000 (RIPA) Annual Report to Standards Committee 2022 and RIPA Inspection

Meeting:	(1) Standards And Audit Committee (2) Cabinet Member for Governance
Date:	(1) 27th July 2022 (2) Tbc
Report by:	RIPA Senior Responsible Officer
For Publication	

1.0 Purpose of Report

1.1 To give an annual report to members on activities relating to surveillance by the Council and policies under the Regulation of Investigatory Powers Act 2011.

1.2 To inform members of the routine RIPA inspection by the IPCO

2.0 Recommendation

2.1 To note the report and the outcome of the 2022 inspection.

2.2 That the Surveillance Policy be updated as set out in this report with the Head of Regulatory Law authorized to make any necessary consequential amendments.

2.3 That the proposed activity for 2022/23 be progressed.

3.0 Reason for recommendations

3.1 To enable the Council to operate the RIPA system effectively and as required by law and guidance.

4.0 Report details

4.1 RIPA

Chesterfield Borough Council has powers under the Regulation of Investigatory Powers Act 2000 (RIPA) to conduct authorised directed surveillances (DI) and use of human intelligence sources (CHIS) in certain circumstances in connection with the conduct of criminal investigations. These powers arise from the need to protect the rights of individuals relating to private and family life (including business relationships).

4.2 Reporting to Members

This report is submitted to members as a result of the requirement to report to members under paragraph 3.35 of the Home Office Code of Practice for Covert Surveillance and Property Interference.

4.3 The previous annual report was submitted to members in April 2019. Due to other priorities, including work arising from the Covid-19 pandemic, no reports were issued in 2020 and 2021. Further reports will continue to be submitted annually whether or not there has been any authorised surveillance.

4.4 The July 2019 inspection outcome was reported to members in September 2019.

4.5 Background

All directed surveillances (covert, but not intrusive) and use of covert human intelligence sources (CHIS) require authorisation by a senior Council officer and the exercise of the powers is subject to review. The controls are in place in accordance with the Human Rights Act, particularly the right to respect for family and private life.

4.6 Originally the Office of the Surveillance Commissioner (OSC) oversaw the exercise by councils of their surveillance powers. However, since September 2017 and the coming into effect of the Investigatory Powers Act 2016 this role is undertaken by the Investigatory Powers Commissioner (IPC)[1]. The Right Honourable Sir Brian Leveson is the current IPC.

4.7 A confidential database of authorised surveillances (the central record) is maintained, charting relevant details, reviews and cancellations. There

[1] https://www.ipco.org.uk/

have been no authorisations since 2010. Because of data retention considerations there is no data contained within the database.

4.8 Substantial changes were made to the powers of Local Authorities to conduct directed surveillance and the use of human intelligence sources under the Protection of Freedoms Act 2012.

4.9 As from 1 November 2012 Local Authorities may only use their powers under the Regulation of Investigatory Powers Act 2000 to prevent or detect criminal offences punishable by a minimum term of 6 months in prison (or if related to underage sale of alcohol and tobacco – not relevant to this Council). The amendment to the 2000 Act came into force on 1 November 2012.

4.10 Examples of where authorisations could be sought are serious criminal damage, dangerous waste dumping and serious or serial benefit fraud. The surveillance must also be necessary and proportionate. The 2012 changes mean that authorisations cannot be granted for directed surveillance for e.g. littering, dog control or fly posting.

4.11 As from 1 November 2012 any RIPA surveillance which the Council wishes to authorise must be approved by an authorising officer at the council and also be approved by a Magistrate; where a Local Authority wishes to seek to carry out a directed surveillance or make use of a human intelligence source the Council must apply to a single Justice of the Peace.

4.12 The Home Office have issued guidance, in the form of codes of practices, to Local Authorities and to Magistrates on the approval process for RIPA authorisations. The most recent code of practice guidance was issued in September 2018 and was considered in the 2019 annual report to this Committee.[2]

5.0 Activity between 2019 and 2022

No directed surveillance

5.1 During this period no directed surveillances (DS) or use of human intelligence sources (CHIS) were authorised by the Council under the Act. The police used Council CCTV for a duly authorised monitoring exercise in 2021, but as this was not a Council investigation RIPA was not engaged for this authority.

[2] https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

Training

5.2 In the 2018 annual report members were informed that an Aspire Learning module covering all key issues of RIPA had been trialled by some enforcement officers and was to be rolled out to all officers involved with enforcement, their managers, relevant legal officers and also the chief executive (who has ultimate responsibility). Further, more detailed, modular training would be considered as and when necessary in due course.

5.3 59 officers involved in enforcement activity are identified as required to complete the mandatory RIPA module in 2022. At the time of writing this report (22nd June 2022) 49 users are certified and 10 are yet to successfully complete the module.

5.4 The 2022 inspection confirmed that there was less stress by the IPCO on training currently, provided relevant officers maintained awareness of RIPA. However, it is not proposed to change the Council requirement for these officers to revisit the training module each year.

5.5 In addition to the RIPA module, the Monitoring Officer, who is the RIPA Senior Responsible Officer, also undertakes external training courses where appropriate.

Internal guidance

5.6 Intended unified guidance on the use of CCTV and e.g. body cams by Council enforcement staff was not developed as intended. This will be carried forward to 2022/23 (see below).

5.7 Following the RIPA inspection in 2019 guidance was published on the Council's intranet[3] including reference to relevant issues and controls relating to:

- Social Media
- Employee monitoring
- Drones
- Error reporting

---

33 https://aspire.interactgo.com/Utilities/Uploads/Handler/Uploader.ashx?area=composer&filename=Regulation+of+Investigatory+Powers+-+2019+Update.pdf&fileguid=0785f79f-314b-4076-b305-1852fafe1248

Governance

5.8 The executive responsibility for the RIPA function is with the Cabinet Member for Governance.

6.0 IPCO Annual Reports

6.1 Each year the Investigatory Powers Commissioner issues comprehensive annual reports to the Prime Minister on all aspects of surveillance, with a section with findings on local authorities. Since the previous annual report to this committee there have been three IPCO annual reports.

6.2 The 2018 Annual Report (published December 2019) related to all surveillance activities and agencies. The section on local authorities recognised the IPCO's

…dual function with regard to local authorities: first, inspecting the recorded use of covert powers and, secondly, investigating the culture and practice across the organisation to establish a level of confidence that any who need to use covert powers would be recognised by staff and would be properly authorised.

6.3 It noted the continuing decline in use of covert powers, with most authorities not using covert powers at all. One reason was that benefit fraud was now being investigated by the DWP, another was that local authorities preferred use of overt investigations and working with the police. Resource limitations also played a part, with the requirement to obtain a magistrates court authorization seen by many to be a hurdle not a safeguard.

6.4 Its findings included that authorizing officers should clearly articulate their considerations relating to necessity, proportionality and collateral intrusion, and that any CHIS application should be accompanied by a risk assessment. It focused on use of social media in investigations and enforcement (see elsewhere in this report and the 2019 inspection) and said it would continue to focus on this activity in 2019, and the importance of regular training.

6.5 The 2019 Annual Report (published October 2020) noted the continued low use by local authorities of RIPA powers for covert surveillance, with the risk of staff becoming less skilled over time and their general fear of incorrect use of the powers. There was an increasing risk of using internet and social media for investigations, with inherent privacy

implications. Investigations were increasingly overt, and due to reduced financial resources authorities often favoured collaborative working instead. The importance of training was again emphasised, as was the need for clear policies on the use of CHIS.

6.6 Use of the internet as a legitimate information source should be used responsibly and in a structured way, and that councils could consider firewalls and permissions systems to prevent unrestricted access to such information. Such use should also be auditable. It recognised the use of mobile and other CCTV as a deterrent (but seeing that authorised covert use could lead to prosecutions and convictions). The risks of staff using private devices for surveillance was highlighted.

6.7 It found an increased use of directed surveillance to detect and prosecute housing fraud, even though this did not reach the crime test in the Protection of Freedoms Act 2012. The report also reviewed the use of communications data by local authorities.

6.8 The 2020 Annual Report (published November 2021) noted the change to using remote inspections during the pandemic and the focus on adequacy of data retention safeguards and proper storage. It recognised the continued low usage of investigatory powers, and the diversion of resources during the pandemic. Innovative use of partnership to reinforce enforcement was supported. It remains unusual for local authorities to use CHIS.

6.9 On use of the internet and social media it noted that overt use of social media monitoring involves data protection issues, overseen by the ICO and that guidance is published by the Home Office. Guidance should be available to staff, online activity should be recorded and periodically scrutinised.. Without an audit trail it is difficult for the SRO to have necessary reassurance that the internet is being used in a controlled and well understood manner.

6.10 Use of surveillance against fly tipping and unauthorised disposal of waste, and to detect RTB fraud was noted. It recognised that in some authorities training paused during the pandemic, but said that it should be resumed. It recognised the benefit of centralised authorisations through the National Anti Fraud Network for acquiring communications data: It made inspection easier (one body rather than hundreds of local authorities, and obviated need for relevant training at those authorities).

6.11 Proper storage of data, review, retention and disposal is stressed. Authorities should consider whether RIPA material should be retained or disposed as soon as it is no longer needed for the authorised purpose or when there are no legal proceedings (something which had been picked up in the April 2020 IPCO letter – see below).

7.0 IPCO Review of Data Handling and Retention Safeguards

7.1 In April 2020 the IPCO issued a letter to public authorities they oversee to help ensure compliance with obligations including the Data Protection Act 2018.

7.2 Their enquiries had found that many authorities held data for longer then necessary or appropriate, partly because data retention and disposal policies were not properly in effect. No decisions were being taken about how long data should be retained in individual cases, and in some cases data was retained indefinitely. Future IPCO inspections would include this aspect. The following was recommended:

- Review safeguarding obligations in the relevant Code of Practice
- Ensure policies for retention, reviewing and disposal of data are accurate and up to date
- Ensure authorising officer has full understanding of any data pathways
- Ensure all data obtained is clearly labelled and stored on a data pathway with a known retention policy
- Review wording of safeguards in any applications to obtain data and ensure they accurately reflect retention and disposal processes
- Review whether data obtained under previous authorisations is being retained for longer than necessary and if necessary consider disposal

8.0 IPCO Inspection 2022

8.1 In September 2019 the outcome of the in-person IPC inspection in July 2019 was reported to members[4]. The inspection report recommended some updates to the Council's surveillance policy which were adopted. It also recommended that officers' personal profiles were not used when conducting online activity.

[4] https://chesterfield.moderngov.co.uk/documents/s27556/Report%20-%20RIPA%20-%20IPCO%20Inspection%20Report%20-%2019-09-25.pdf

8.2 The next three year inspection was through a Teams interview on 9th June 2022. This was a desktop inspection between the inspector and the RIPA Senior Responsible Officer, also attended by the Data Protection Officer.

8.3 During the inspection the inspector confirmed that the absence of annual reviews during the pandemic was not exceptional or problematic, and mirrored other authorities, not least as investigation activity would have been restricted during this period, which included lockdowns.

8.4 The inspector was complimentary about the Council's RIPA Policy and considered it one of the best they had seen.

8.5 They advised that IPCO emphasis had changed from RIPA training to a more general awareness of likely circumstances where RIPA related considerations might arise.

8.6 They referred to the IPCOs April 2020 data handling letter and that the authority's central record should refer to the need to hold data no longer than necessary and in accordance with retention and disposal policies. Some minor updates to the RIPA policy were discussed, including emphasis on officers not using personal accounts for social media.

8.7 Sir Brian Leveson's written inspection report, dated 13th June, found:

- That the Council had made the necessary arrangements in response to the 2019 inspection report, and discharged the recommendations made.
- That the Council's RIPA policy was impressive, covered most relevant points and was easy to follow
- Some minor amendments/inclusions were recommended to the policy (these are incorporated in the amended RIPA Policy attached)
- While noting that no activity had been conducted, it was important to ensure there was an awareness of RIPA across the organisation, and noted the online training module available to staff
- Clear guidance was contained in the policy regarding management of the product of surveillance, also included in the Information Asset Register
- That the Council was well placed to comply with safeguarding provisions in the Codes of Practice, and might consider adapting the Central RIPA record to include management and review of such product if acquired.

9.0 Surveillance Policy and other updates

9.1 The Council's RIPA Policy is available on the Council's website and here. In spring 2022 it was updated to:

- remove reference to Arvato and Kier (the partnership ending there was no longer the need to note separate regimes) and
- reflect changes in some service and post names.

9.2 The policy has now been updated in draft to reflect the recommendations of the 2022 inspection and any relevant issues in the Annual Reports and April 2020 IPCO letter on data retention as well as more general updates (See Appendix).

9.3 The RIPA Central Record has been amended to refer to data retention and disposal requirements.

10.0 Activity in the current year

10.1 While the authorisation process is very rarely appropriate or necessary and has not been used since 2010 the 2022 inspection indicates that the council is well placed should any be required.

10.2 A RIPA update will be sent to relevant officers.

10.3 Updated information will be placed on the RIPA and other pages of the Council's intranet, as necessary.

10.4 Relevant corporate CCTV policy and guidance is still to be developed. This will include the use of body cams by Council enforcement staff and deployable cameras. The growth in use of CCTV by different services, whilst overt surveillance, requires greater consistency across the authority and a corporate CCTV policy should be developed.

11.0 Alternative options

11.1 Given the outcome of the 2022 inspection and the current position on directed surveillance, no alternatives are appropriate.

12.0 Implications for consideration – Financial and value for money

12.1 The inspection outcome endorses the Council's approach to RIPA.

13.0 Implications for consideration – Legal

13.1 The RIPA system sets up a framework for surveillance which needs to be properly followed. The Council has not needed to carry out authorized covert surveillance in recent years.

14.0 Implications for consideration – Human resources

14.1 N/A

15.0 Implications for consideration – Council plan

15.1 The Council's RIPA policy and practices contribute to improving the quality of life for local people

16.0 Implications for consideration – Climate change

16.1 There are not considered to be any direct climate change impacts in relation to this report.

17.0 Implications for consideration – Equality and diversity

17.1 N/A

18.0 Implications for consideration – Risk management

18.1 Proper application of the surveillance policy will help to minimize risks arising on this matter.

Decision information

Key decision number	*N/A*
Wards affected	All

Document information

Report author
Gerard Rogers Head of Regulatory Law and Monitoring Officer – RIPA Senior Responsible Officer

Corporate	
Background documents These are unpublished works which have been relied on to a material extent when the report was prepared.	
This must be made available to the public for up to 4 years.	
Appendices to the report	
Appendix 1	Surveillance Policy – with tracked amendments