

OFFICIAL- SENSITIVE

DISCLAIMER

This report contains the observations and recommendations identified by an individual surveillance inspector, or team of surveillance inspectors, during an inspection of the specified public authority conducted on behalf of the Chief Surveillance Commissioner.

The inspection was limited by time and could only sample a small proportion of covert activity in order to make a subjective assessment of compliance. Failure to raise issues in this report should not automatically be construed as endorsement of the unreported practices.

The advice and guidance provided by the inspector(s) during the inspection could only reflect the inspectors' subjective opinion and does not constitute an endorsed judicial interpretation of the legislation. Fundamental changes to practices or procedures should not be implemented unless and until the recommendations in this report are endorsed by the Chief Surveillance Commissioner.

The report is sent only to the recipient of the Chief Surveillance Commissioner's letter (normally the Chief Officer of the authority inspected). Copies of the report, or extracts of it, may be distributed at the recipient's discretion but the version received under the covering letter should remain intact as the master version.

The Office of Surveillance Commissioners is not a public body listed under the Freedom of Information Act 2000, however, requests for the disclosure of the report, or any part of it, or any distribution of the report beyond the recipients own authority is permissible at the discretion of the Chief Officer of the relevant public authority without the permission of the Chief Surveillance Commissioner. Any references to the report, or extracts from it, must be placed in the correct context.

OFFICIAL – SENSITIVE



OSC/INSP/075

Office of Surveillance
Commissioners

The Rt. Hon. Lord Igor Judge
Chief Surveillance Commissioner
Office of Surveillance Commissioners
PO Box 29105
London
SW1V 1ZU

22nd July 2016

OSC INSPECTION – SOUTH RIBBLE BOROUGH COUNCIL

Inspector

Graham Wright – Surveillance Inspector

Introduction

1. South Ribble Borough Council is a small district council serving a mixed urban and rural population in Lancashire. The principal centres of population are Leyland and the southern suburbs of Preston.
2. The previous OSC inspection was conducted in September 2013 by Sir David Clarke, Assistant Surveillance Commissioner.
3. The Chief Executive of South Ribble Borough Council is Mike Nuttall whose address for correspondence is The Civic Centre, West Paddock, Leyland, Lancashire PR25 1DH. Mr Nuttall was in post at the time of the last inspection.
4. South Ribble's RIPA 'senior responsible officer' (SRO) is Mr Ian Parker who was not in post at the time of the previous inspection.
5. Since the last inspection there have been no RIPA authorisations of directed surveillance or covert human intelligence sources (CHIS).
6. I am preparing this report without visiting South Ribble Borough Council. Having considered this material in detail, I have concluded that I can properly report to you without a physical inspection. This is in accordance with your recent direction that not every second-tier district or borough council needs to be visited every three years as a matter of course.

Progress against recommendations/Action Plan

7. The one recommendation made in 2013 related to changes required in the main policy document in respect of the detail provided as to when a member of the public might be a CHIS and the removal of references to urgent oral authorisations. The required changes have been made and the Governance Committee were informed of the OSC Inspection outcome and the action taken in relation to it.

OFFICIAL - SENSITIVE

PO Box 29105 London SW1V 1ZU Tel 020 7035 8127 Fax 020 7035 3114

Web: <https://osc.independent.gov.uk> email: oscmmailbox@osc.gsi.gov.uk

RIPA Structure and Policy

8. Mr Ian Parker, the Director of Governance and Business Transformation is the appointed 'senior responsible officer'. Mr David Whelan, Legal Services Manager, undertakes the role of RIPA Administrative Officer and has responsibility for day to day activity conducted under the Act and would maintain the Central Record of authorisations, should any be granted – the last one was in 2008. I examined a copy of the Record. This is in the form of a hard-copy register and needs to have additional information included to comply with the requirements of the Code of Practice.¹ **I make a recommendation in this regard.**
9. The Legal Services Team has close working relationships with all enforcement departments/units and their advice is sought on many aspects of investigations, not just RIPA.
10. There are three designated authorising officers, this includes the Chief Executive.
11. The main policy document is the *Policy Statement – RIPA 2000* (July 2016) and this is a clear, thorough and useful document. The changes required by the recommendation of 2013 have been completed. There is a brief section on 'Social Networking Sites and the Internet' which is largely accurate. The only reservation that I have is that the section states, "where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required." The first part of this sentence may be true, such data may be considered as open source but it is inaccurate to say that an authorisation is not usually required without the caveat that the repeat viewing of open source sites may constitute directed surveillance on a case by case basis.²
12. The above document is supplemented by the *Social Media Protocol* (June 2013) which contains advice regarding how employees should use these media in a proper manner.
13. This second document does not really add any further clarity regarding Council staff using SNS and the internet to gather information in support of their council functions and as we have found in inspections recently such use is frequent and is often done with a lack of awareness regarding how such usage might be an infringement of a person's privacy. This situation is further complicated by the fact that departments not usually associated with the conducting of covert activity, i.e. Human Resources and Children's and Adult Services, are making use of these media. The challenge for councils is to have appropriate and accurate guidance and ensure that all staff are made aware of that guidance. **I make a recommendation in this regard.**

Reports to Members

14. Reports are given to the Governance Committee but given the infrequent usage of RIPA these reports are done on an annual basis. OSC inspections are fully reported upon.

¹ Paragraph 8.1 of the Covert Surveillance Code of Practice refers.

² Note 289.1 of OSC Procedures and Guidance 2016 refers.

Liaison with magistrates' court under The Protection of Freedoms Act 2012

15. The policy document referred to at paragraph 11 above contains a description of the process to be followed and the active involvement of the Legal Services Manager. A solicitor would attend any such hearing along with the applicant.

Training

16. All officers from Environmental Health (the main enforcement department) have in the past 2-3 years undertaken training in investigative techniques and this course included a substantial input on RIPA. It is intended that a further training event regarding RIPA will be convened following this inspection process, and incorporating any learning points from the inspection.
17. It does not appear that any other training has occurred and notwithstanding the high standards and knowledgeable officers, I advise that there should be periodic awareness and refresher training. The SNS and internet issue makes this even more important.

Social media investigations

18. I mention at paragraph 13 above the need for more comprehensive guidance and training to a wide audience of council staff. I have been informed that there is a good level of understanding among 'relevant officers' regarding this issue and staff are encouraged to speak to Legal officers. Because of our findings in inspections we are tending to encourage a more proactive response; namely, carrying out an audit of usage among even those departments that are not the traditional investigative or enforcement units. The vulnerability for the council is that *'they don't know what they don't know'* and this activity is so easy to carry out by anyone with access to electronic data equipment.

CCTV

19. There are only 13 fixed site cameras in the Council area. The viewing room is not staffed, footage is only viewed if an incident occurs and there is never pre-planned usage of the cameras in circumstances which would meet the requirement for an authorisation for directed surveillance.

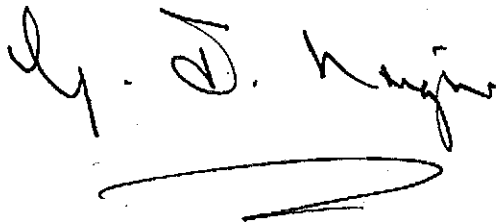
Conclusions

20. South Ribble Borough Council continues to make no use of the powers vested under Part II of the Regulation of Investigatory Powers Act 2000 and in response to the request for information stated that the culture of the organisation is to use overt methods only.
21. This does not negate the need for a clear and accurate policy and guidance regime; indeed the need for such guidance is at least equal to that needed in an authority that makes regular use of RIPA. This is particularly true in relation to use of the internet and social networking sites which is an area of concern for the OSC. This concern is due to several factors: because of the ease by which such covert activity can be conducted; a lack of thorough understanding among staff as to when a subject's privacy might be interfered with; and the fact that usage of these media is far wider than those staff traditionally associated with conducting covert activity.

22. The other recommendation that I make is in relation to the Central Record of authorisations which, albeit dormant for over eight years, requires some emendation to record all the information as prescribed in the Code of Practice.

Recommendations

23. The format of the Central Record of authorisations should be emended to include all the information required by paragraph 8.1 of the Covert Surveillance Code of Practice – paragraph 8.
24. An audit should be carried out to ascertain the extent of usage of the internet and SNS, suitable awareness training provided to staff and the main policy document should be amended to include the fact that repeated viewing of open source material may constitute directed surveillance and should be considered, in an informed manner, on a case by case basis – paragraphs 11 to 13 and 18.

A handwritten signature in black ink, appearing to read 'G. D. Hargrave', with a large, sweeping underline.

Surveillance Inspector