



Investigatory Powers  
Commissioner's Office

PO Box 29105, London  
SW1V 1ZU

Angela Scott  
Chief Executive  
Aberdeen City Council  
Marischal College  
Aberdeen  
AB10 1AB

[anscott@aberdeencity.gov.uk](mailto:anscott@aberdeencity.gov.uk)

23 June 2020

Dear Chief Executive,

### Inspection of Aberdeen City Council

*Please be aware that IPCO is not a "public authority" for the purpose of the Freedom of Information (Scotland) Act (FOISA) and therefore falls outside the reach of the FOISA. It is appreciated that local authorities are subject to the FOISA and that they may receive requests for disclosure of our reports. In the first instance the SRO should bring the matter to the attention of the IPCO Data Protection Officer (at: [info@ipco.org.uk](mailto:info@ipco.org.uk)), before making any disclosure. This is also the case if you wish to make the content of this letter publicly available.*

Due to the ongoing Coronavirus situation your authority was recently subject to a remote inspection by one of my Inspectors, [REDACTED]. All the documentation and arrangements necessary for my Inspector to carry out the process was provided by Ms. Jess Anderson, Team Leader, Legal Services who acts as the RIP(S)A Co-ordinator for your authority. This enabled an examination of all relevant policies and an assessment of the progress made against the three recommendations from the last inspection in April 2017. Ms. Anderson also made herself available to be interviewed at length via telephone by [REDACTED] and from the documentation examined and the information provided during the telephone interview, the very good level of compliance shown by your authority removes, for the present, the requirement for a physical inspection.

At the last inspection your authority received three formal recommendations, and I note from the information provided by Ms Anderson significant effort has been made to ensure measures were implemented to enable these recommendations to be discharged. In relation to recommendation 1, I must compliment the process you now have in place to report to Elected Members in line with the requirements of the relevant codes of practice<sup>1</sup>. The process you have, in reporting annually and on a quarterly basis to your Audit, Risk and Scrutiny Committee, is exactly as required by the codes of practice. The standard of these reports, particularly that produced to the committee in February this year, was exemplary and is one that is worthy of sharing to a wider audience. My Inspector was very impressed by the attitude of Ms. Anderson who, not only being very enthusiastic and knowledgeable on matters related to RIP(S)A, demonstrated a very proactive and innovative approach to governance and oversight of any use, or potential use, of the powers. This process is clear evidence of the pride she takes in her role as RIP(S)A Co-ordinator.

---

<sup>1</sup> Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017, para. 4.43 and Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017, para. 3.27

The maintenance of your central record of authorisations, the advice function provided by Legal Services, and the introduction of quarterly governance meetings involving the Authorising Officers has also been observed as being good practice. At the most recent meeting a demonstration was given by the Principal Trading Standards Officer (PTSO) of the capability of the surveillance equipment held by the Council. This is a practice worthy of praise given the importance of Authorising Officers being able to consider the risk of using technical surveillance equipment and how it may impact on collateral intrusion, and the need to make knowledgeable determinations around that risk when considering directed surveillance applications. I also note that as a result of this meeting it is intended to implement measures to make the asset management processes of surveillance equipment more robust and to be linked more widely with your Information Asset Register.

This inspection has highlighted other notable areas of good practice, including the development of a programme of RIP(S)A training and awareness raising, a full revision of protocols and procedures in line with the potential for an increased use of the internet and social media as an investigative resource, and the very innovative introduction of a restricted [REDACTED] web portal. [REDACTED] was permitted access to the Knowledge Hub web portal and was hugely impressed by the potential this resource has in delivering real benefit to practitioners. Possessing the capability to provide web-based training, the storage of reports and hosting a knowledge sharing portal which allows the speedy distribution of key guidance will no doubt, as the resource develops, improve staff awareness and the skills of your practitioners. It was clearly apparent that Ms Anderson has a real passion in delivering this function for the Council and again demonstrative of the commitment she has towards RIP(S)A compliance.

Recommendation 3 from 2017 related to the policy you maintained, like some other local authorities, of not affording the protection of RIP(S)A to test purchase operations where council operatives may enter premises to provide corroboration of the transaction. I note that in each case where this tactic was deployed, a total of nine occasions since the last inspection, each instance was afforded the protection of RIP(S)A by a directed surveillance authorisation, each authorised for the statutory period of three months. It is true that each case should be considered upon its own merits and the nature of the deployment and, whilst being a policy decision for you, the approach you have taken allows this recommendation, and recommendation 2, to be discharged.

I note that Ms Anderson has placed considerable focus on assessing the potential use of the internet and social media across various business areas within the Council to ensure it has robust oversight measures in place and that appropriate guidance is maintained in that regard. A separate appendix, *'Using Social Media as an Investigatory Tool'*, is now attached to your *Corporate Protocol and Procedures on Directed Surveillance* which is a good quality document providing scenario-based examples to practitioners in cases where RIP(S)A may require to be considered. It must be noted that both current Scottish Government Codes of Practice contain enhanced guidance at paragraphs 3.11 to 3.16<sup>2</sup> and 4.7 to 4.14<sup>3</sup> and it may benefit the document if staff are signposted to these sections. Ms. Anderson has intimated that this topic will feature prominently in the programme of training under development, and given the privacy risks attached to the use of social media as an investigative resource, it is very important such guidance is reinforced to uphold the obligations towards the rights afforded to citizens under Article 8 of the European Convention on Human Rights (ECHR).

In discussion with Ms. Anderson it was abundantly clear she was alive to the possibility of the potential of online social media research being carried out in respect of Council priorities which would not generally be within the purview of RIP(S)A. She has already embarked on wider awareness raising of the issue, and it is important that regardless of the reasons for conducting such research, employees are reminded of the obligations public authorities have to the Article 8 Rights of individuals, and of the need to demonstrate legitimate and proportionate reasons for carrying out online research.

---

<sup>2</sup> Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017

<sup>3</sup> Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

The Investigatory Tribunal's decision in *BA & others v Chief Constable of Cleveland IPT/11/129/CH (13 July 2012)* was highlighted to Ms. Anderson where the IPT commended the adoption in non-RIPA cases "a procedure as close as possible" to that required by the legislation. A documented record and audit trail would reduce the risk of there being a disproportionate use of social media in these circumstances and helps ensure legitimate aims are being pursued. It is also important that the policies you have in place highlight to staff the dangers aligned to using personal social media accounts for business purposes, especially those of a covert nature, and that they are cognisant of their own personal online security and of the vulnerabilities attached to using any insecure or personal online platform.

RIP(S)A permits your authority to recruit and authorise CHIS, and whilst there appears to be no real appetite for the use of CHIS, good guidance is available to practitioners within section 6 of your protocol outlining the principles underpinning the tactic. It is to your credit that awareness of the tactic is delivered to staff, and that your PTO has some operational experience of CHIS, which is important in enabling staff to be conscious of situations where potential considerations of CHIS may be necessary. You have included an appendix within your protocol, '*Identifying when a Human Source becomes a CHIS*', which is a very useful document to help achieve this type of operational awareness. Some good examples of situations are described in paragraphs 2.18, 2.23 and 2.25<sup>4</sup>, the highlighting of which within your policy would benefit staff who may interact with members of the public who offer information, particularly those who may do so repeatedly, and where it may be necessary for them to give some consideration to the guidance within the code of practice.

The *Corporate Protocol and Procedures on Directed Surveillance* has been very recently updated by Ms. Anderson and shared with my Inspector. The protocol takes account of the changes in the legislation, as well as the introduction of revised Scottish Government codes of practice in December 2017. My Inspector has commented on the considerable work undertaken by Ms. Anderson in developing the protocol to make it more meaningful to staff by incorporating relevant scenario examples, process flow charts, and an outline of the identified training requirements and the training programme, which no doubt will benefit your staff should situations arise where they contemplate the use of covert tactics.

I am aware that you have received my letter dated 1<sup>st</sup> May 2020 outlining IPCO's Data Assurance Programme and that Ms. Anderson is already placing significant focus on the issue and reviewing the processes in place for those business areas which may make use of covert powers. It appears that she is very much in control of the issue and it is encouraging that the most recent revisions in the protocol incorporate guidance on the storage, management and retention of material obtained as a result of covert tactics. This topic was discussed at length during the remote inspection and it was emphasised as being an area of compliance which IPCO will focus on more deeply in future inspections. The relevant sections of Chapter 8 within each of the Scottish Government Codes of Practice on Covert Surveillance and Property Interference and Covert Human Intelligence Sources are appropriately referenced within your policies and it is important that practitioners are fully cognisant of their responsibilities in this regard.

Oversight continues to be a strength within your authority with your RIP(S)A Coordinator taking an extremely proactive and intrusive approach ensuring that there is regular engagement with Authorising Officers regardless of the level of use of the powers. This is an area of good practice demonstrative of a positive and robust attitude to compliance, and my Inspector has commented in very complimentary terms on the extremely high level of professionalism and commitment Ms. Anderson displays to this aspect of her role within the authority, and given the relatively small part it plays in her wider role in Legal Services, she should be commended for that.

---

<sup>4</sup> *Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017*

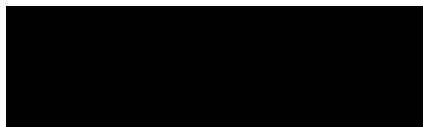
I note your authority is not registered to use the services of the National Anti-Fraud Network (NAFN), and it is suggested that a short statement to this effect is included within the review of your RIP(S)A policy. That said, changes to communications data powers available to local authorities brought about by the Investigatory Powers Act 2016 are considerable and may be of real investigative benefit. The primary purpose of NAFN is to acquire communications data which now includes events data (who a person has been in communications with), as well as where that communication was made or received. In addition, registration with NAFN can provide lawful access to other forms of data from the DVLA, Equifax and a variety of other financial/fraud check organisations, and might also include, in the future, Automated Number Plate Recognition (ANPR) data.

In conclusion, it must be emphasised that despite making very limited use of any powers, it is vital that the relevant staff are appropriately trained should the need arise to authorise and carry out covert activity. Given that your authority's attitude to training and oversight is strong, I am confident the development of your training programme will ensure that officers engaged in investigatory or enforcement areas can maintain their levels of knowledge and know whom to approach for guidance. The RIP(S)A Coordinator, on behalf of the SRO, has given assurances that the integrity of your processes and governance procedures will be maintained to ensure that high standards of compliance with the Act and relevant codes of practice continue to be achieved.

I am sure you will be pleased that elements of good practice have been identified, and that you have a RIP(S)A Co-ordinator who possesses such commitment to her role. I would highlight that any observations made are designed to assist your organisation and enable your staff to be more efficient in their respective roles whilst applying the legislation to covert investigative techniques.

I hope that you find the outcome of this remote inspection helpful and constructive, and my Office is available to you should you have any queries following the receipt of this letter, or at any point in the future. Contact details are provided below. I shall in any case, be interested to learn of your proposed response to any of the observations made within the attached report within the next two months.

The Inspector would like to thank Ms. Jess Anderson for her very positive engagement and for providing the necessary documentation to enable this remote inspection.

A large black rectangular redaction box covering the signature of the Investigatory Powers Commissioner.

**The Rt. Hon. Sir Brian Leveson**  
The Investigatory Powers Commissioner