



Investigatory Powers
Commissioner's Office

PO Box 29105, London
SW1V 1ZU

Roddy Burns
Chief Executive
The Moray Council
High Street
Elgin
Moray
IV30 1BX

██████████@moray.gov.uk

5 May 2021

Dear Chief Executive,

IPCO Surveillance and CHIS Inspection of Moray 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), 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 pandemic your authority was recently subject to a remote inspection by one of my Inspectors, ██████████. The documentation and arrangements necessary for my Inspector to carry out the process was provided by ██████████ Head of Economic Growth and Development, who acts as your Senior Responsible Officer (SRO). This enabled an examination of relevant policies and two of the authorisations (CHIS and directed surveillance authorisation) granted since the last inspection in November 2018. ██████████ made himself available to be interviewed via video conferencing, and from the documentation examined and the information provided during the interview, the level of compliance shown by your authority removes, for the present, the requirement for a physical inspection.

At the last inspection your authority was subject to two recommendations, and I note from the information provided that in response to Recommendation 1 you implemented a Training Register in 2019, which enables this recommendation to be discharged. I am aware though that opportunities to deliver appropriate training has been limited, not least by the impact of the pandemic. I note from the discussion with ██████████ that the Council continues to hold the RIPS Forum which was highlighted as good practice in the last inspection. I am aware that this function enables additional oversight to be applied to the use of the powers by the SRO, and once again I would encourage this type of forum as being good practice.

I understand that opportunities will be sought to deliver appropriate training to staff once COVID restrictions are lessened, and whilst I am conscious that your authority's usage of covert powers is low, I would emphasise the importance of ensuring staff are appropriately trained should the need arise to authorise and carry out covert activity. I am confident, given the commitment shown by the SRO to ensure adequate training is delivered, that your staff will be able to maintain their knowledge levels and general RIPSAs awareness.

Recommendation 2 related to revising the policy of an Authorising Officer occupying the role of SRO. I note that [REDACTED] no longer performs the role of Authorising Officer and as such, can operate with some independence whilst discharging the role of SRO in accordance with paragraphs 4.42¹ and 9.2². I am therefore able also to discharge Recommendation 2.

In relation to the requirements contained within paragraphs 4.43³ and 3.27⁴ to ensure Elected Members have oversight of the authority's use of RIPSAs, I note that the last submission to the Policy and Resources Committee was in May 2018. I am aware that there is an intention to submit an updated report to the Committee in June 2021 and, whilst I acknowledge this intention, I would remind you of the requirements outlined in the codes of practice. You will also note the relevant paragraphs outline good practice for Public Authorities to consider reporting use of RIPSAs on a quarterly basis, particularly if they use the powers frequently.

My Inspector has commented favourably on the policy and guidance documents you have in place to provide staff appropriate direction on the use of the powers attached to CHIS and covert surveillance. Not only are they made available on the Council intranet, but they have been published on the public facing Council website which illustrates an attitude of openness and transparency. [REDACTED] has indicated that the guidance offered is appropriate to your use of the powers, and has been updated to take account of the latest versions of the codes of practice. Whilst the policy and the *Pre-Surveillance Checklist* do provide adequate guidance, they may benefit from signposting staff to relevant sections within the codes of practice, and to some of the operational examples contained therein. The provision of examples and scenarios will no doubt assist staff in being able to apply considerations around RIPSAs within an operational context.

[REDACTED] also opines that the policy would benefit from additional detail and guidance being provided to staff around the use of the internet and social media as part of investigations which attract the risk of interference with the Article 8 Rights of individuals. It is important that staff are aware of these risks and of the proper procedure attached to the use of this tactic. It is good practice for all members of staff, regardless of regulatory function, to be aware of the guidance around these tactics and to be 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 where breach of privacy is a risk.

It is important that the use of social media and the internet is appropriately overseen and audited within all public authorities, regardless of whether it can be afforded the protection of RIPSAs or not. In that regard, the Investigatory Powers Tribunal's decision in *BA & others v Chief Constable of Cleveland IPT/11/129/CH (13 July 2012)* was discussed with your officers. The IPT commended the adoption in non-RIPAs (RIPSAs) 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 good practice to highlight to staff the dangers of using personal social media accounts for business purposes, especially those of a covert nature, and to make them aware of their own personal online security and of the vulnerabilities of using any insecure or personal online platform.

¹ Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017

² Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

³ Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017

⁴ Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

My Inspector has examined one CHIS use and conduct authorisation and one directed surveillance authorisation granted since the last inspection, upon which he makes the following general points:

1. Applicants do well in providing sufficient and specific information outlining the background of the investigation, which allows the requisite elements of necessity, proportionality and collateral intrusion to be considered against the nature of the tactic being sought, as per paragraph 5.4⁵ and 5.10⁶.
2. Operational objectives outlined in CHIS applications are of a good standard.
3. Risk assessments attached to CHIS authorisations are appropriate and highlight the relevant risks attached to deployments, in line with paragraph 6.12⁷.
4. Authorising Officers should articulate their considerations around collateral intrusion when authorising directed surveillance and CHIS, as per paragraphs 4.9 to 4.15⁸ and 3.9 to 3.12⁹.
5. Authorising Officers should ensure that they are specific in terms of the activity and conduct they are authorising, as per paragraphs 4.8¹⁰ and 3.8¹¹ and the obligations laid down by *R v SUTHERLAND*¹².
6. Cancellations should provide detail on what activity has been undertaken, the type and extent of the product and material obtained, and how it is to be managed, with the Authorising Officer providing some direction or instruction for its management.

He also makes positive comment that the authorisation of CHIS in the operational circumstances described is in line with the provisions outlined in paragraph 2.15¹³, and appropriately takes into account the risk attached to your officers having to establish a relationship with sellers beyond an offer to buy counterfeit goods in order to achieve an operational outcome.

RIPSA permits your authority to recruit and authorise CHIS from the community, and whilst there has been no use of CHIS in these circumstances, it is important that staff are sufficiently knowledgeable to be conscious of situations where potential considerations of CHIS may be necessary. Some good examples of situations are described in paragraphs 2.18, 2.23 and 2.25¹⁴, 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.

I am aware that you have received my letter outlining IPCO's Data Assurance Programme and that your guidance policies contain distinct sections to cover the *Security and Retention of Documents*. I would point you to the relevant sections within the codes of practice and to the principles of Data Assurance contained within my letter, and suggest replicating aspects of the guidance and principles within your policies to ensure appropriate safeguards are applied. This is an area of compliance which IPCO will focus on more deeply in future inspections, and whilst the physical practices could not be tested on this occasion, some additional guidance will enable practitioners to understand fully their responsibilities.

⁵ Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017

⁶ Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

⁷ Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

⁸ Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017

⁹ Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

¹⁰ Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017

¹¹ Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

¹² *R v SUTHERLAND (2002) EW Misc 1 (EWCC)*

¹³ Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

¹⁴ Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017

I am pleased to report there being suitably strong governance processes in place within your Council to ensure compliance with the legislation and codes of practice, and I would highlight the observations made herein 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 note your authority is registered with the services provided by the National Anti-Fraud Network (NAFN), although has made no use of the available services.

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 this letter within the next two months.

The Inspector would like to thank [REDACTED] for his enthusiastic engagement with the remote inspection process, and for providing the necessary documentation to enable it to be achieved.

Yours sincerely,

A black rectangular redaction box covering the signature of the sender.

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