The Use of Investigatory Powers Policy

Approved by Audit, Risk and Scrutiny Committee on 2 December 2021 with an implementation date of 2 December 2021

ABERDEEN
CITY COUNCIL

Document Control

Approval Date	2 December 2021
Implementation Date	2 December 2021
Policy Number	Request from Assurance Team
Policy Author(s) and Owner	Jess Anderson, Fraser Bell
Approval Authority	Audit, Risk and Scrutiny Committee
Scheduled Review	12 months
Date and Changes: 28 Sept 2021 – Policy Group Review 5 Oct 2021- Risk Board Review and approval Dec 2021- Committee approved policy	

Table of Contents

1 Why does the Council need this Policy?

1.1 There are a range of situations in which Council officers in the course of their duties have to carry out investigations and activities for legitimate purposes and it's deemed necessary and proportionate to use investigatory powers to acquire information about a person, either in their personal capacity or about their trade or business.

1.2 The Council's policy documents are control documents designed to mitigate risks. Policies are key controls in the Council's Risk Management Framework. This policy sets out the monitoring and assurance framework (such as a robust application/ authorisation process, audits, training and awareness raising provided by Legal Services) around the Council's use of specific investigatory techniques and powers by trained officers to enforce statutory duties the Council is tasked with discharging. By doing so, this policy mitigates any potential risks in relation to an unlawful interference with a person's right to a private and family life under the Human Rights Act 1998 (HRA)[1], and ensures that the Council and its officers have clarity on the reporting arrangements in respect of this type of activity.

1.2 In particular, this policy ensures the Council complies with the requirement in the Scottish Government's "Covert Surveillance and Property Interference Code of Practice" and "Covert Human Intelligence Sources Code of Practice" that elected members set the policy for covert surveillance activity on an annual basis and ensure it remains fit for purpose. Additionally, this policy harmonises the assurance and monitoring in place for covert surveillance and extends that to situations where authority to acquire Communications data is sought and obtained.

1.3 In setting policy each year, members are giving that formal endorsement that the arrangements in place, and monitored by the Chief Officer- Governance as Senior Responsible Officer (SRO), comply with the relevant legislation through practical application of the operational procedures, training and awareness raising.

2 Application and Scope Statement

2.1 The Council does, and shall, continue to use the powers available to it under the Investigatory Powers Act 2016 (IPA) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) respectively, as key investigation tools where it has a lawful purpose to do so. This policy relates to the Council's use of covert surveillance and the acquisition of Communications data and defines the control environment and principles around the use of such investigatory powers. This policy does not extend to officers who do not have an investigatory or enforcement role whereby this type of activity is a real likelihood, nor does it apply to any external or partner organisations.

[1] Article 8 of the HRA.

2.2 The Council has specific powers under RIPSA, to conduct Directed Surveillance and it may authorise the use of a Covert Human Intelligence Source (CHIS) (where it is deemed necessary and proportionate). Directed Surveillance is surveillance for a specific investigation or operation, is covert, and is likely to result in the obtaining of private information about an individual. A CHIS is essentially an undercover officer. The purpose of a CHIS is to establish or maintain a false personal relationship with others to obtain or access information covertly. Covert Surveillance is covert where it is carried out in such a way that anyone subject to it is unaware that the surveillance is taking place. An example of when the Council may use surveillance is to covertly record Trading Standards test purchasing.

2.3 The acquisition of Communications data is permitted by the IPA. Communications data is the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication.

2.4 Any officer requiring to use investigatory powers for a lawful purpose must be trained to do so, prior to applying for, using, and/ or authorising the use of investigatory powers. The operational procedures, referred to at section 4 of this policy, set out the training plan for covert surveillance and the acquisition of Communications data. Further, Authorising Officers are required to attend the same training prior to authorising an application for the use of investigatory powers and attend/ participate in quarterly meetings. Sections 1.3 and 1.4 of this policy set out the role which Elected Members play in setting policy.

2.5 The Council has entered into a contract with the National Anti-Fraud Network (NAFN) who provide assurance and advice to council officers where there is a lawful purpose to access Communications data. It is a requirement of the IPA that the Council has a person/ organisation in place to undertake this role. NAFN is the only provider approved by the Home Office to carry out these services.

3 Responsibilities

3.1 The Chief Officer - Governance as SRO is responsible for this policy. The SRO is the main point of contact for the Council with the Investigatory Powers Commissioner (IPC), the Office for Communications Data Authorisations, and the Home Office. The SRO is responsible and answerable to the IPC for the Council's compliance in respect of the use of these investigatory powers. The SRO has delegated powers to appoint

Authorising Officers for covert surveillance and Designated Senior Officers for the acquisition of Communications Data. The SRO shall continue to report to the Audit Risk and Scrutiny Committee on a quarterly basis on covert surveillance activity, and he shall also report on Communications data activity in so far as it does not impact on operational matters.

3.2 The Council is also required to appoint a Designated Senior Officer(s) (DSO) for Communications data purposes. This person(s) has delegated authority to authorise an application for such data. Details of the DSO are included within the operational procedure and on the restricted online forum referred to at section 4.2 below.

3.3 A willful breach of this policy by any Council officer shall be considered a disciplinary matter and will be dealt with under the Council's agreed disciplinary procedures or as a contractual dispute where the breach was caused by a third party engaged by the Council in the acquiring of Communications data. Further, a breach of this policy and supporting procedures may also be a breach of Data Protection Legislation and be reported and investigated internally having regard to the Corporate Information Policy and supporting Information Handbook of procedures. These responsibilities are highlighted in the training provided on the use of these investigatory powers.

3.4 As noted at 2.6 above, the Council contracts with NAFN to carry out the role of a Single Point of Contact (SPoC). The SPoC is there to ensure that any applications for the acquisition of Communications data are practical and lawful. The SPoC also provides objective judgement and advice to the Council and the Protective Services Manager on the application.

3.5 The Regulatory and Compliance (R&C) Team, Legal Services monitor compliance regarding covert surveillance activity and Communications data requests. Primarily this is done by maintaining a central record for covert surveillance and Communications data activity. Access to this record is restricted to the R&C Team and this record includes every application, authorisation or refusal made by the Council. The R&C Team also provides regular awareness raising, on the quality of applications/ authorisations (in respect of covert surveillance only), and training to officers.

4 Supporting Procedures & Documentation

4.1 This policy is supported by two operational procedures**: namely Covert Surveillance and the Acquisition and Retention of Communications Data.** These procedures govern how applications and authorisations for the use of investigatory powers shall be made, reviewed and cancelled. They also set out how any data obtained shall be used, kept, accessed and destroyed, having particular regard to Data Protection Legislation and Data Assurance. They are available on the Council's intranet along with this policy. A copy of this policy is available on the Council's intranet.

4.2 Officers who have received training on **Covert Surveillance** and/or the **Acquisition and Retention of Communications Data** will be provided with access to an online restricted forum where these procedures, guidance, news/updates and application/ authorisation forms (for covert surveillance only) will be accessible. This online resource was developed and is maintained by the R&C Team.

4.3 The Chief Officer – Governance has the power under the Council's Scheme of Governance to approve any necessary changes to the procedures referred to in 4.1 above. At all times, the procedures will be consistent with the terms of this Policy.

4.4 Any changes to process, or law shall be notified to officers through the online forum (referred to at 4.2 above), and amendments to this policy or the procedures shall be uploaded after approval, so that the information available on that forum is up to date and accurate at all times.

5 About this Policy

5.1 This policy demonstrates the Council's intention to exercise the powers available to it under the IPA and RIPSA and provides a framework to ensure that the powers are exercised in accordance with the law.

6 Risk

6.1 This policy and its supporting procedures will manage the following risks:

- **Compliance Risks** - The policy and supporting documentation will reduce the risk of non-compliance with the Human Rights Act 1998, IPA and RIPSA, by setting out the standards and behaviours required in order to ensure compliance. This policy sets out how routine monitoring is in place to ensure continued compliance with these documents and the relevant legislation.

- **Reputational Risks** – The policy and supporting documentation sets out the standards required when considering and applying to use these investigatory powers. Failure to report to committee on covert surveillance activity and follow procedure could lead to reputational damage when this is identified by the IPC at their inspection. This risk is mitigated by reporting to the Audit, Risk and Scrutiny Committee on a quarterly basis. Further, any IPC inspection report is shared with Committee and any resultant action plan is endorsed by Committee.

- **Operational Risks** – the policy and supporting documentation sets out the process all Council officers must follow when they wish to use investigatory powers under the IPA and RIPSA. Further, it is a requirement of this policy that officers receive training prior to applying to use investigatory powers. Officers who have not been trained shall not be permitted to use the investigatory powers referred to under this policy. This risk is managed by managers highlighting which staff require training due to their enforcement/ investigatory roles. Awareness-raising in this regard and the wider impact of surveillance work is done on a biennial basis.

7 Environmental Considerations

7.1 This policy does not relate to, nor have an impact on, any environmental factors. As such an Environmental Assessment was not undertaken.

8 Policy Performance

8.1 Setting policy is a requirement under the Code of Practice on Covert Surveillance and Property Interference. Assurance that the policy is effective when conducting covert surveillance falls to the Audit, Risk and Scrutiny Committee. Covert surveillance activity has been reported regularly to this committee since Autumn 2017 and it is considered prudent to extend that oversight role to the acquisition of Communications data, albeit such extension is not a statutory requirement. The effectiveness of this policy will be demonstrated by the feedback during inspections undertaken by the IPC but also in the quarterly reporting on the use of these powers to this Committee and compliance with this policy and its operational procedures. Committee will continue to receive updates on the use of investigatory powers on a quarterly basis.

8.2 The R&C Team, Legal Services undertake audits of all authorisations of covert surveillance applications and feedback is provided to council officers. Additionally, the R&C Team will maintain a record of all applications where these are made, refused or authorised, reviewed, renewed and/or cancelled in respect of both covert surveillance and the acquisition of Communications data. Additionally, any errors made by the Council under the IPA are reported to the Chief Officer- Governance. Collectively, this gives assurances that the policy is performing well, as there is a framework to mitigate and manage non- compliance.

8.3 The Investigatory Powers Commissioner (IPCO) has oversight of the Council's use of investigatory powers under the IPA and RIPSA by way of an inspection every 3 or 4 years. The IPC focuses on the Council's compliance under those legislative regimes. As a matter of course, the IPC reviews the Council's policy and any feedback on its

performance, clarity or meaning would be reflected in the IPC inspection report which this Committee will be sighted on.

9 Design and Delivery

9.1 This policy links to the Aberdeen City Local Outcome Improvement Plan (LOIP), particularly the stretch outcomes; Prosperous Economy and Prosperous Place. The LOIP states that "All people in Aberdeen are entitled to live within our community in a manner in which they feel safe and protected from harm", and "promote wellbeing and good health choices/ to nurture our physical health". The use of investigatory powers, where this is appropriate, in tackling offences such as the selling of counterfeit goods or routine test purchases of tobacco related products to ensure they are being sold in accordance with the law, demonstrates the Council's commitment to these outcomes and that it will act, where it is empowered to do so.

9.2 Council's Statutory Obligations - this policy links to the Council's statutory obligation not to act in a way which is incompatible with a human right, under section 6 of the HRA.

10 Housekeeping and Maintenance

10.1 This policy shall be reviewed annually by the Audit, Risk and Scrutiny Committee. The procedures which support this policy shall follow the same review timeline, so that changes or amendments to policy flow through to the procedures, where this is necessary.

10.2 The SRO as Chief Officer - Governance has delegated powers under the Council's Scheme of Governance, Powers Delegated to Officers [2] to create and amend procedures, protocols and guidance. Any changes or amendments required will be referred to the SRO for approval.

11 Communication and Distribution

11.1 This policy will be uploaded to the Covert Surveillance page on the intranet, with a link provided from the Leadership Forum, and it will also be available on a restricted online forum. Access to this forum has been given to all staff who have completed the training.

11.2 Further, specific training will also be provided for any officer who requires to work with this policy, and guidance and support shall be provided on an ongoing basis.

[2] PDO

12 Information Management

12.1 Any personal information gathered as a result of an officer using investigatory powers shall be processed in compliance with the Data Assurance practices and Data Protection Legislation, as set out in the supporting procedures.

Definitions

Communications data	means the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication;
Data Protection Legislation	means the (i) "UKGDPR" being the retained EU law version of the General Data Protection Regulation ((EU) 2016/679) as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018 and as amended by Schedule 1 to the Data Protection, Privacy and the Electronic Communications (Amendments etc) (EU Exit) Regulations 2019 (SI 2019/419) and any applicable national implementing Laws as amended from time to time; and (ii) the Data Protection Act 2018 to the extent that it relates to the processing of personal data and privacy;
Covert Surveillance	means surveillance by way of either Directed Surveillance or a Covert Human Intelligence Source undertaken for a specific purpose or investigation and in a manner that is likely to result in the obtaining of private information about any person.
Data Assurance	means the way in which the Council, officers and elected members understand and have clarity about what happens to information about, and obtained as a result of, using investigatory techniques.