

## **REPORT TO BUSINESS SERVICES COMMITTEE – 15 NOVEMBER 2018**

### **ANNUAL REPORT OF ACTIVITY UNDER THE REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000 POLICY**

#### **1 Recommendations**

**The Committee is recommended to:**

- 1.1 Consider and comment on the annual report of activity under the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) Policy at Appendix 1; and**
- 1.2 Agree the revised policy on Authorisation of Surveillance under the Regulation of Investigatory Powers (Scotland) Act 2000, at Appendix 2.**

#### **2 Background / Discussion**

- 2.1 On 22 June, 2017, following the outcome of an inspection by the Office of the Surveillance Commissioner, the Committee approved a revised policy on the authorisation of surveillance under RIPSA.
- 2.2 The Scottish Government Code of Practice for Covert Surveillance and Property Interference calls for local authorities to have elected member oversight of any activity in connection with RIPSA. Accordingly, at its meeting on 16 November, 2017, the Committee agreed to receive annual reports on RIPSA activity under the policy in order to scrutinise the Council's use of surveillance powers and ensure compliance with the Code of Practice.
- 2.3 The annual report for 2017/2018 forms Appendix 1. It summarises the use of surveillance over the previous twelve months and details any changes in legislation or notable cases on the use of RIPSA. Having considered the terms of the annual report, officers from Legal and Governance are satisfied that only minor amendments to the policy are required at this stage, as detailed in paragraph 2.4. The Committee will continue to receive quarterly bulletins which will alert members to any issues surrounding the policy and a further annual report will follow in November, 2019.
- 2.4 A minor amendment is required to the policy on Authorisation of Surveillance under the Regulation of Investigatory Powers (Scotland) Act 2000 to amend the officer responsible for maintaining the Council's Central Register to "Laura Bremner" from "Robin Taylor". Further, at page one of the policy, a definition of what may constitute private information has been inserted to provide greater clarity. The revised policy forms Appendix 2 to this report.
- 2.4 The Head of Finance and Monitoring Officer within Business Services have been consulted in the preparation of this report, had no comments to make and are satisfied that the report complies with the Scheme of Governance and relevant legislation.

### **3 Scheme of Governance**

- 3.1 The Committee is able to consider and take a decision on this item in terms of Section C.1.1.g of the List of Committee Powers in Part 2A of the Scheme of Governance as it has responsibility for Legal and Governance, which, in turn, has responsibility for the policy on Authorisation of Surveillance under RIPSA.

### **4 Implications and Risk**

- 4.1 An equality impact assessment is not required because there are no direct material outcomes from this report and the proposals do not have a differential impact on any of the protected characteristics.
- 4.2 There are no staffing and financial implications arising from this report.
- 4.3 The following Risks have been identified as relevant to this matter on a Corporate Level:-

ACORP002 – Regular reporting of activity will ensure Members are advised timeously of any changes to national policy, legislation and regulation that may impact on Council policy, enabling appropriate action to be taken.

ACORP006 – Reputation Management: Failure to take action to comply with the Code of Practice and recommendations by the Office of the Surveillance Commissioner could result in the Council being criticised in future inspection reports.

### **Ritchie Johnson, Director of Business Services**

Report prepared by Ruth O'Hare, Principal Solicitor and Laura Bremner, Principal Solicitor  
Date: 25 October, 2018

**APPENDIX 1**  
**ANNUAL REPORT**  
**ON THE USE OF THE REGULATION OF INVESTIGATORY POWERS**  
**(SCOTLAND) ACT (RIPSA) 2000**

1. Between 1 October 2017 and 1 October 2018, Aberdeenshire Council granted four authorisations for the use of directed surveillance under the 2000 Act. Three of the authorisations granted related to the sale of nicotine products to under 18s and one of the authorisations granted related to the sale of counterfeit goods.
2. Between 1 October 2017 and 1 October 2018, Aberdeenshire Council granted two authorisations for the use of a covert human intelligence source (CHIS). One of the authorisations granted was in relation to cigarettes and the other related to designer goods.
3. During the period 1 October 2017 to 1 October 2018, there have been no reported cases on the operation of RIPSA and there have been no legislative changes to the Act.
4. The new Codes of Practice on the use of RIPSA came into force on 28 February 2018. The Council's policy on surveillance has been reviewed in light of the new Codes of Practice and, though no strictly changes are necessary, it is considered that clarification on what is classed as "private information" would assist.
5. In January 2018, The Investigatory Powers Commissioner advised that he was very pleased to note that the detailed Action Plan drawn up in July 2017 had been completed, to the extent that the recommendations from the Council's 2014 and 2017 inspections had been satisfactorily addressed and that there is a clear intention to continue to maintain the required readiness to be able to use the RIPSA powers of directed surveillance and CHIS should the need arise in future, together with reports to the Council's elected members on a regular basis. Given the response to previous inspection findings and the requests of the Chief Surveillance Commissioner, the Investigatory Powers Commissioner advised that he was satisfied that there would be no need for Aberdeenshire Council to be inspected again in 2018.

## APPENDIX 2

### Policy on Authorisation of Surveillance under the Regulation of Investigatory Powers (Scotland) Act 2000

#### Introduction

1. In some circumstances it may be necessary for Council employees in the course of their duties to make observations of a person or persons in a covert manner i.e. without that person's knowledge. By their nature actions of this sort are potentially intrusive (in the ordinary sense of the word) and may give rise to legal challenge as a potential breach of Article 8 of the European Convention of Human Rights and the Human Rights Act 1998 ("the right to respect for private and family life").
2. The Regulation of Investigatory Powers Act 2000 [RIPA] and the Regulation of Investigatory Powers (Scotland) Act 2000 [RIP(S)A] ("the Acts") together provide a legal framework for covert surveillance by Public Authorities and an independent inspection regime to monitor these activities. The Regulation of Investigatory Powers Act 2000 provides for the acquisition of communications data by local authorities in Scotland. Its provisions regarding covert surveillance apply only to England.
3. The Scottish Government has produced codes of practice on Covert Surveillance and the use of Covert Human Intelligence Sources ("the Codes of Practice"). This document should be read in conjunction with the Codes of Practice to ensure that all covert surveillance by Council employees is carried out effectively while remaining in accordance with the law.
4. This procedure only applies where surveillance is covert. It does not apply to observations or surveillance that is not carried out covertly nor does it apply to unplanned observations made as an immediate response to events. Surveillance using CCTV cameras which are visible and which are accompanied by notices advising of their presence is overt and will not require authorisation whereas using hidden cameras or in circumstances where the presence of CCTV is not made clear to those who might be affected is covert and will require authorisation.
5. This procedure and the Acts do not permit authorisation by Aberdeenshire Council Officials of intrusive surveillance i.e. covert surveillance carried out in relation to anything taking place on residential premises or in any private vehicle which involves the presence of an individual on the premises or in the vehicle or which is carried out by means of a surveillance device.
6. This procedure applies where directed surveillance or use of a covert human intelligence source is to be used.

#### Directed Surveillance

7. This is covert but not intrusive and is undertaken for the purpose of a specific investigation or specific operation in such a manner as is likely to result in the obtaining of private information about a person. Private information includes

any information relating to the person's private or family life and may include personal data such as names, phone numbers and address details.

### **Covert Human Intelligence Source**

8. This is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of either using the relationship to obtain information or to provide access to any information to another person or disclosing information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. It would be unusual for the Council to use a Covert Human Intelligence Source.

### **Principles of Surveillance**

9. In planning and carrying out covert surveillance Aberdeenshire Council employees shall comply with the following principles: -
10. **Lawful purposes** – covert surveillance shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in the Acts) i.e. it must be:-
  - for the purpose of preventing or detecting crime or the prevention of disorder
  - in the interests of public safety
  - for the purpose of protecting public health
11. **Necessity** – Covert Surveillance shall only be undertaken where there is no other reasonable and effective way of achieving the desired objective(s). It is necessary for the applicant for a surveillance authorisation to set out who is to carry out the surveillance, when it will be done, how it will be done, what is being investigated and the grounds on which the surveillance is being carried out, including, where known, the identities of those subject to the surveillance. This must be considered on a case by case basis.
12. **Effectiveness** – planned covert surveillance shall be undertaken only by suitably trained or experienced employees or under their direct supervision.
13. **Proportionality** – the use and extent of covert surveillance shall not be excessive i.e. it shall be in proportion to the significance of the matter being investigated. The least invasive method of investigation that will enable the aim of the surveillance to be achieved should be adopted. All other practicable, less intrusive steps should have been taken and surveillance authorised only as a last resort.
14. **Collateral Intrusion** – reasonable steps shall be taken to minimise the acquisition of personal information that is not directly necessary for the purposes of the investigation or operation being carried out. Employees carrying out surveillance shall not cause damage to any property or harass any person. This should be considered as part of the proportionality principle. Employees should not carry out surveillance from private property without the consent of the occupier.

15. **Authorisation** – all surveillance shall be authorised in accordance with the procedures described below.
16. **Confidential Material** – includes matters subject to legal privilege, confidential personal information and confidential journalistic material. Personal information includes information relating to a person's physical or mental health, or spiritual or other counselling received by a person. Information is held in confidence if it is held under an express or implied undertaking to hold it in confidence, or if it is subject to a restriction on disclosure or obligation of secrecy contained in existing or future legislation. Such material should not be copied or retained unless it is necessary for a specific purpose. Such material should be disseminated only where an appropriate officer, having taken legal advice, is satisfied that it is necessary for a specific purpose. Any retention or dissemination of such material should be accompanied by a clear warning of its confidential nature. Reasonable steps should be taken to ensure that there is no possibility of it becoming available, or its contents becoming known, to any person whose possession of it may prejudice any related criminal or civil proceedings. Such material should be destroyed as soon as it is no longer necessary to retain it for a specified purpose. If there is any doubt about the status of the material, legal advice should be sought before further dissemination.

### **The Authorisation Process**

17. **Directed Surveillance** – The persons who may authorise applications are detailed in Appendix III. Authorisation levels are prescribed by the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Order 2000. In relation to Local Authorities, the Regulations refer to Assistant Head of Service and Investigation Manager, titles which are little used within Councils. The Authorisation levels set by the Council are equivalent to or above those, and also reflect best practice that there should be at least two organisational tiers of separation between the Applicant and the Authorising Officer. Applicants should apply within their own line management structure unless other arrangements have been agreed or it is unreasonable or impractical in the circumstances.
18. Applications will normally be made in writing using the approved form. The Applicant must provide information about the investigation or operation to be carried out and must state who is to be carrying out the surveillance, when it will be done, how it will be done, against whom and what is being investigated and the offence being prevented/detected. In urgent cases, oral or written applications may be approved by any Authorising Officer. Where an urgent application is made this should be supplemented by a normal written application as soon as practicable and in any event within 72 hours failing which the authorisation will expire.
19. Before the Application can be granted, the Authorising Officer must be satisfied that the grant is in accordance with the Principles of Surveillance as detailed above, that it is necessary, that the action is proportionate to what it seeks to achieve and that the aim could not have been achieved by other means. The Authorising Officer must state explicitly and in his/her own words what is being authorised, and against which subjects, property or location.

Mere reference to the terms of the application is inadequate. The Authorising Officer must also note the time and date of the grant/refusal of the Application on the relevant form.

20. Where there is a significant risk of confidential material being recovered, the Application shall require the approval of the Chief Executive or in his absence, a Director. Where the majority of the information likely to be recovered could be confidential, the Application should only be granted in exceptional and compelling circumstances.
21. An authorisation for Directed Surveillance runs for a period of three months from the date of grant of the authorisation but should be issued only for the period in which it is expected the surveillance operation will take place.
22. All authorisations shall be reviewed by the Authorising Officer at intervals of not more than four weeks. Details of said review and the decision reached shall be noted on the original application.
23. An application for renewal of the authorisation of directed surveillance can be made at any stage using the appropriate form. The authorisation must be cancelled at any stage if the person who granted or last renewed an authorisation is satisfied that the authorised conduct no longer satisfies the purpose for which it was granted or the requirements regarding necessity, proportionality and collateral intrusion are no longer met. The cancellation of the authorisation should be recorded on the appropriate form. When cancelling an authorisation, the Authorising Officer should:
  - Record the date and times (if at all) that surveillance took place and the order to cease the activity was made.
  - The reason for cancellation.
  - Ensure that surveillance equipment has been removed and returned.
  - Provide directions for the management of the product.
  - Ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded.
  - Record the value of the surveillance or interference (i.e. whether the objectives as set in the authorisation were met).
24. **Covert Human Intelligence Source** –The process for the grant of authorisation for the use or conduct of a Covert Human Intelligence source is the same as for Directed Surveillance. The Authorising Officer must state explicitly and in his/her own words what is being authorised, and against which subjects, property or location. Mere reference to the terms of the application is inadequate. The application for use or conduct of a Covert Human Intelligence Source must specify who the controller and who the handler is to be for each Source. In addition, authorisation for use of a Covert Human Intelligence Source can only be granted after a risk assessment on the use of a Covert Human Intelligence Source and if sufficient arrangements are in place for handling the source's case the risk assessment should determine the risk to the Source of carrying out actions and the likely

consequences should the role of the source be known. The ongoing security and welfare of the Source after the cancellation of the Authorisation should also be considered prior to granting the Application. The arrangements that are considered necessary are that:-

25. There will at all times be a person holding the requisite office, rank or position with the relevant investigating authority who will have day to day responsibility for dealing with the source on behalf of that authority and for the source's security and welfare – this should be the source's line manager (the Handler).
26. That there will at all times be another person holding the requisite office, rank or position with the relevant investigating authority who will have general oversight of the use made of that source – this should be the handler's line manager (the Controller).
27. That the identity of the Handler and the Controller for each Source will be set out in the Application.
28. That there will be at all times a person holding the requisite office, rank or position with the relevant investigating authority who will have responsibility for maintaining a record of the use made of that source – this should be the Authorising Officer
29. That the record relating to the use of that source are maintained by Aberdeenshire Council which will always contain particulars of such matters as may be specified in regulations made by the Scottish Ministers.
30. That the records maintained by Aberdeenshire Council that discloses the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.
31. The persons who may authorise applications are detailed in Appendix III.
32. The Chief Internal Auditor is not an Authorising Officer for this type of surveillance.
33. Only the Chief Executive (or in his absence a Director) can authorise the use of a Covert Human Intelligence Source who is a vulnerable individual or a juvenile.
34. Authorisation for the conduct or use of a Covert Human Intelligence Source runs for 12 months beginning with the date the authorisation takes effect. Authorisation of the use of a Covert Human Intelligence Source who is a vulnerable individual or a juvenile runs for one month.
35. All authorisations shall be reviewed by the Authorising Officer at intervals of not more than four weeks. Details of said review and the decision reached shall be noted on the original application.

36. Applications for the renewal of the conduct or use of a covert human intelligence source shall not be granted unless the officer is satisfied that a review has been carried out of the use made of the source in the period since the grant, the task given to the source during that period and the information obtained from the conduct or use of the source and has considered the results of such a review. The authorisation must be cancelled if the person who granted or last renewed an authorisation is satisfied that the authorised conduct no longer satisfies the purpose for which it is granted. When cancelling an authorisation, the Authorising Officer should:
- Record the date and times (if at all) that surveillance took place and the order to cease the activity was made.
  - The reason for cancellation.
  - Ensure that surveillance equipment has been removed and returned.
  - Provide directions for the management of the product.
  - Ensure that detail of property interfered with, or persons subjected to surveillance, since the last review or renewal is properly recorded.
  - Record the value of the surveillance or interference (i.e. whether the objectives as set in the authorisation were met).

### **Documents**

37. This procedure uses the following documents (list of forms detailed in Appendix II): -
38. Application for Authorisation to carry out Directed Surveillance [Form 1] - this should be completed by the applicant in all Directed Surveillance cases. The Authorisation is effective from the time that the approval was given, which should be noted on the Form by the Authorising Officer.
39. Review of a Directed Surveillance Authorisation [Form 2] - this should be used to record the reviews specified in the initial Form 1.
40. Application for Renewal of Directed Surveillance Authorisation [Form 3] - this should be completed by the applicant in all cases where surveillance is required beyond the previously authorised period (including previous renewals).
41. Cancellation of a Directed Surveillance Authorisation [Form 4] - this should be completed either by the Applicant or the Authorising Officer when the authorisation ceases to be necessary or appropriate. The Authorising Officer must sign the Cancellation form.
42. Application for Authorisation for Use or Conduct of Covert Human Intelligence Source [Form 5] - this should be completed by the applicant in all CHIS cases not covered by oral authorisation (below). The Authorisation is effective from the time that the approval was given, which should be noted on the Form by the Authorising Officer.
43. Review of a Covert Human Intelligence Source Authorisation [Form 6] - this should be used to record the reviews specified in the initial Form 5.

44. Application for renewal of a Covert Human Intelligence Source Authorisation [Form 7] - this should be completed by the applicant in all cases where surveillance is required beyond the previously authorised period (including previous renewals).
45. Cancellation of Authorisation for Use or Conduct of Covert Human Intelligence Source [Form 8] - this should be completed either by the Applicant or the Authorising Officer when the authorisation ceases to be necessary or appropriate. The Authorising Officer must sign the Cancellation form.
46. Covert Surveillance – Oral Authorisation [Form 9] - this is a record of an oral authorisation which should be completed by the applicant. It should be used only where the urgency of the situation makes the submission of a written application prior to commencement of the surveillance impractical. It should be countersigned by the original authorising officer as soon as is practical. An Application in either Form 1 or Form 5 requires to follow within 72 hours.
47. Each form must be completed with a Service Identifier, a Location Identifier and a reference number unique to that application. The Service Identifiers to be used are contained in Appendix I. The reference number should start with the Service Identifier, thereafter it is up to each Service to decide how best to ensure that all documentation is readily available and identifiable. Each application will also be allocated with a Central reference number by the Head of Legal and Governance.

#### **Review of Authorisations**

48. All authorisations shall be reviewed by the Authorising Officer at intervals of not more than four weeks. Details of said review and the decision reached shall be noted on the original application.

#### **Security and Retention of Documents**

49. Documents created under this procedure are highly confidential and shall be treated as such. The Head of Legal and Governance shall maintain one Central Register of current and past Authorisations at Woodhill House. Where an application for Authorisation is granted renewed or cancelled, the Applicant officer shall telephone or e-mail the officer responsible for maintaining the Central Register, and also send a copy of the grant, renewal or cancellation to the Head of Legal and Governance, both within 24 hours of same to keep the Central Register up to date. The Central Register shall contain the following information, namely :-
  - the type of authorisation;
  - the date the authorisation was given;
  - name and rank/grade of the authorising officer;
  - the unique reference number (URN) of the investigation or operation;
  - the title of the investigation or operation, including a brief description and names of subjects, if known;
  - whether the urgency provisions were used, and if so why;
  - if the authorisation has been renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer;

- whether the investigation or operation is likely to result in obtaining confidential information;
  - whether the authorisation was granted by an individual directly involved in the investigation;
  - the date the authorisation was cancelled.
50. The principal Authorisation and Renewal forms shall be retained by the Authorising Officer while current. On cancellation, the principal Application, Renewal and Cancellation forms shall be forwarded to the Head of Legal and Governance with the Authorising Officer retaining a copy.
51. Said forms shall be retained by the Authorising Officer for at least one year after cancellation and by the Head of Legal and Governance for at least five years after cancellation.
52. All information recovered through the use of covert surveillance which is relevant to the investigation shall be retained for at least five years after the cancellation of the surveillance or the completion of any Court proceedings in which said information was used or referred to. All other information shall be destroyed as soon as the surveillance is cancelled.

### **Training**

53. Each Service is responsible for ensuring that their staff receive adequate training to deal with applications and enquiries. The Director of each Service shall confirm to the Head of Legal and Governance that appropriate staff have received training in the interpretation of the legislation, codes and forms and provide details, including the date(s), of the training.

### **Public Access**

54. Copies of the Policy and the Codes of Practice are available for public reference at the following offices:-
- Woodhill House, Westburn Road, Aberdeen.
  - St. Leonards, Sandyhill Road, Banff.
  - Gordon House, Blackhall Road, Inverurie.
  - Viewmount, Arduthie Road, Stonehaven.
55. Copies of the Policy and the Codes of Practice will be made available to the public by post or e-mail if requested.

### **Complaints**

56. In the event of any member of the public being unhappy or dissatisfied with the conduct of any covert surveillance, in addition to the Council's complaints procedure, they have the right to complain to the Investigatory Powers Tribunal.
57. Details of the Complaints Procedure are available for public reference at the above offices. Copies of the Complaints Procedure will be made available to the public by post or e-mail if requested.

**APPENDIX I**

Service Identifiers:-

BS – Business Services

CE – Chief Executive

ECS -Education and Children's Services

HSC – Health and Social Care

IS - Infrastructure Services

LG – Legal and Governance

**APPENDIX II**

**Form 1 – Application for Authorisation to carry out Directed Surveillance**

**Form 2 – Review of a Directed Surveillance Authorisation**

**Form 3 – Application for Renewal of Directed Surveillance Authorisation**

**Form 4 – Cancellation of Directed Surveillance Authorisation**

**Form 5 – Application for Authorisation for Use or Conduct of Covert Human Intelligence Source**

**Form 6 - Review of Covert Human Intelligence Source Authorisation**

**Form 7 – Renewal of Covert Human Intelligence Source Authorisation**

**Form 8 Cancellation of an Authorisation for Use or Conduct of Covert Human Intelligence Source.**

**Form 9 - Covert Surveillance - Oral Authorisation**

**APPENDIX III**

Persons who may grant Authorisations:-

James Savege – Chief Executive

Ritchie Johnson – Director of Business Services

David Hughes – Chief Internal Auditor

Wilma Urquhart – Trading Standards Manager

Officer responsible for maintaining Central Register – Laura Bremner – Legal and Governance.