**Item: 8**

**Policy and Resources Committee: 16 June 2026.**

**Regulation of Investigatory Powers and Covert Surveillance.**

**Report by Chief Executive.**

ORKNEY ISLANDS COUNCIL

# 1. Overview

1.1. This report updates Members on the processes that require to be followed by local authorities in connection with the exercise of their statutory powers to conduct covert surveillance. It advises of the outcome of the most recent review by the Investigatory Powers Commissioner's Office of the Council's compliance with the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) and the Investigatory Powers Act 2016, attached as Appendices 1 – 2 of this report. The report further notes the work undertaken to review and update relevant policies and procedures to comply with best practice and seeks Members' approval of the updated policies and procedures attached as Appendices 3 - 7 of this report.

**Statutory Regulation and Oversight**

1.2. In accordance with the Scottish Government Covert Surveillance and Property Interference Code of Practice and Covert Human Intelligence Sources Code of Practice, the policies and procedures of a local authority relating to its use of covert surveillance, including directed surveillance, and the use of covert human intelligence sources, require to be reviewed annually. This last review was completed in September 2025.

1.3. Since September 2025, there have been no changes in legislation or to relevant guidance in connection with the Council's statutory powers to conduct covert surveillance, and there has been no need for the Council to conduct covert surveillance or otherwise use these powers.

**Review Process and Outcomes**

1.4. In January 2026, the Investigatory Powers Commissioner's Office requested the Council to complete and submit an update on its compliance with relevant legislation, in line with the requirement that it has to carry out an investigation into Council compliance every three years. Following this investigation process, the Investigatory Powers Commissioner's Office confirmed that they were satisfied with the Council's compliance. They made a single suggestion for enhancement of the Council's Surveillance through Social Media Policy, which is addressed in this report, and advised that no further inspection would be required until 2029.

**Review of Policies and Procedures**

1.5. In order to ensure best practice, the Council's existing policies and procedures in connection with the Council's arrangements for covert surveillance have been reviewed and are presented for consideration.

1.6. Following the review, and in light of the enhancement suggested by the Investigatory Powers Commissioner's Office, an update to section 8 of the Surveillance through Social Media Policy is proposed. This update provides that a request for authorisation shall be submitted whenever there is to be directed online surveillance of an individual's activity that is likely to result in obtaining private information, irrespective of that individual's privacy settings. The proposed updated Surveillance through Social Media Policy is attached as Appendix 7 to this report for the consideration of Elected Members.

1.7. Subject to the update referred to above, in the absence of any further recommendations by the Investigatory Powers Commissioner's Office, or any amendments to legislation or guidance since the last review, no further revisions to the Council's existing policies and procedures in connection with the Council's arrangements for covert surveillance or the use of covert human intelligence sources are proposed.

1.8. The following policies and procedures are accordingly presented for approval and are attached as Appendices 3 – 7 of this report:

- Policy on Covert Surveillance.
- Procedure for Authorisation of Covert Surveillance.
- Policy on Use of Covert Human Intelligence Sources.
- Procedure for Authorisation of the Use of Covert Human Intelligence Sources.
- Surveillance through Social Media Policy, including proposed updates in Section 8.

## 2. Recommendations

2.1. It is recommended that members of the Committee:

i. Note that the Investigatory Powers Commissioner's Office has confirmed their satisfaction with the Council's compliance with all relevant requirements relating to the Regulation of Investigatory Powers (Scotland) Act 2000 and the Investigatory Powers Act 2016 and that there will be no further inspection required until 2029.

ii. Note the enhancement suggested by the Investigatory Powers Commissioner's Office in respect of Section 8 of the Council's Surveillance through Social Media Policy and the update that is being proposed in response.

iii. Approve the existing policies and procedures in connection with the Council's arrangements for covert surveillance and the use of covert human intelligence sources, attached as Appendices 3 – 6 to this report, and the updated Surveillance through Social Media Policy, attached as Appendix 7 to this report.

## 3. Background

3.1. In terms of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA), the Council can carry out covert surveillance:

- For the purposes of preventing or detecting crime or the prevention of disorder.
- For the purposes of protecting public health.
- In the interests of public safety.

3.2. Examples of how the Council may carry out covert surveillance include:

- To investigate complaints of anti-social behaviour.
- To investigate breaches of certain types of legislation (for example, Trading Standards and Environmental Health legislation).
- To investigate fraudulent benefit claims.

3.3. Covert surveillance includes directed surveillance, which is a covert surveillance undertaken for the purposes of a specific investigation or operation in a manner that is likely to result in the obtaining of private information about a person.

3.4. A covert human intelligence source is a person who establishes or maintains a personal relationship with another person for the purpose of either covertly using the relationship to obtain information or to provide access to any information to another person, or covertly disclosing information obtained by the use of such a relationship.

3.5. In accordance with the Covert Surveillance and Property Interference Code of Practice and the Covert Human Intelligence Sources Code of Practice, both issued by the Scottish Government, the policies and procedures of a local authority in relation to its use of covert surveillance, including directed surveillance, and the

use of covert human intelligence sources, require to be reviewed by Elected Members annually.

## 4. Review by Investigatory Powers Commissioner's Office

4.1. On 9 January 2026, the Investigatory Powers Commissioner's Office advised the Chief Executive that the Council was due its three-yearly inspection regarding compliance with RIPSA and the Investigatory Powers Act 2016, noting that the last inspection had taken place in June 2023.

4.2. Following a review of how the Investigatory Powers Commissioner's Office conducts its oversight of local authorities, it no longer routinely undertakes an inspection as had previously been the case. Instead, the Investigatory Powers Commissioner's Office has agreed that each local authority should provide a written update, in the first instance, on its compliance with the legislation. This will enable the Investigatory Powers Commissioner's Office to assess whether or not a remote, or in some cases, in-person inspection is required.

4.3. This is a risk-based approach based upon assessment of risk by the Investigatory Powers Commissioner's Office and ensures that its limited resources are best directed for the coming year.

4.4. The Council was required to submit evidence covering the following:

- Policies and Procedures.
- Training.
- Use of social media.
- Compliance with the relevant Codes of Practice in relation to the Council's retention, review and destruction of material obtained through the use of covert powers.

4.5. On 16 April 2026, Sir Brian Leveson, the Investigatory Powers Commissioner, wrote to the Chief Executive advising that he was satisfied that the Council's response provided assurance that ongoing compliance with RIPSA and the Investigatory Powers Act 2016 would be maintained and that, as such, the Council would not require further inspection until 2029.

4.6. Accompanying the above letter was an email from John Coull, Inspector at the Investigatory Powers Commissioner's Office, to the Head of Corporate Governance, advising that he had found the Council's documents to be comprehensive, detailed and compliant with the relevant requirements. The Inspector made a single

suggestion for enhancement of the Council's Surveillance through Social Media Policy, which is addressed in Section 5 of this report.

## 5. Review of Policies and Procedures

5.1. The Council currently has a number of existing policies and procedures, as follows:

- Policy on Covert Surveillance.
- Procedure for Authorisation of Covert Surveillance.
- Policy on Use of Covert Human Intelligence Sources.
- Procedure for Authorisation of the Use of Covert Human Intelligence Sources.
- Surveillance through Social Media Policy.

5.2. Although the Council rarely uses its statutory powers in respect of RIPSA, it is important that the Council adheres to its statutory obligations and seeks to apply recommendations or observations on good practice made by the Investigatory Powers Commissioner's Office in the exercise of its statutory powers.

5.3. Accordingly, the Council's Surveillance through Social Media Policy has been enhanced in light of an observation by the Inspector at the Investigatory Powers Commissioner's Office that a directed surveillance may be invoked when activity is focused on an individual, takes place repeatedly over a period, and is likely to result in obtaining private information, irrespective of privacy settings. In order to address this observation, an update is proposed to the Policy to provide that, whenever there is to be targeted surveillance of an individual that is likely to result in obtaining private information, a request for a RIPSA authorisation shall be sought, irrespective of the individual's privacy settings and their posts being public.

5.4. Subject to the update referred to above, the position is that there have been no changes in the law or to relevant guidance in connection with the Council's statutory powers to conduct covert surveillance since the Council's existing policies and procedures were last reviewed by the Policy and Resources Committee on 23 September 2025. In addition, since the review last year, there has been no cause for the Council to exercise any of its statutory powers to conduct covert surveillance.

5.5. Accordingly, no amendments to the Council's existing policies and procedures in connection with the Council's arrangements for covert surveillance and the use of covert human intelligence sources are proposed, save for the aforementioned enhancement to the Surveillance through Social Media Policy.

**For Further Information please contact:**
Gavin Mitchell, Head of Corporate Governance, extension 2233, Email: gavin.mitchell@orkney.gov.uk

**Implications of Report**

1. **Financial –** None arising from this report. All costs incurred in respect of RIPSA will be met from existing budgets.
2. **Legal –** See section 3 above.
3. **Corporate Governance –** In accordance with the Code of Practice published by the Scottish Government, a local authority's RIPSA policies and procedures require to be reviewed annually.
4. **Human Resources –** None arising from this report.
5. **Equalities –** An Equality Impact Assessment has been undertaken and is attached as Appendix 6.
6. **Island Communities Impact -** As the policies being reviewed in terms of this report have been assessed as being unlikely to have an effect on an island community which is significantly different from its effect on other communities (including other island communities) in Orkney, a full Island Communities Impact Assessment has not been undertaken.
7. **Links to Council Plan:** The proposals in this report support and contribute to improved outcomes for communities as outlined in the following Council Plan strategic priorities:
   ☐Growing our economy.
   ☒Strengthening our communities.
   ☐Developing our Infrastructure.
   ☐Transforming our Council.
8. **Links to Local Outcomes Improvement Plan:** The proposals in this report support and contribute to improved outcomes for communities as outlined in the following Local Outcomes Improvement Plan priorities:
   ☐Cost of Living.
   ☐Sustainable Development.
   ☒Local Equality.
   ☐Improving Population Health.
9. **Environmental and Climate Risk –** Not applicable.
10. **Risk –** Not applicable.
11. **Procurement –** Not applicable.
12. **Health and Safety –** Not applicable.
13. **Property and Assets –** Not applicable.
14. **Information Technology –** Not applicable.
15. **Cost of Living –** Not applicable.

**List of Background Papers**

Scottish Government Covert Surveillance and Property Interference: Code of Practice.
Scottish Government Covert Human Intelligence Sources: Code of Practice.

**Appendices**

Appendix 1: Letter dated 16 April 2026 from Investigatory Powers Commissioner to Chief Executive.
Appendix 2: Email dated 16 April 2026 from Investigatory Powers Commissioner's Office CHIS and Surveillance Inspector to Head of Corporate Governance.
Appendix 3: Policy on Covert Surveillance.
Appendix 4: Procedure for Authorisation of Covert Surveillance.
Appendix 5: Policy on Use of Covert Human Intelligence Sources.
Appendix 6: Procedure for Authorisation of the Use of Covert Human Intelligence Sources.
Appendix 7: Updated Surveillance through Social Media Policy.
Appendix 8: Equality Impact Assessment.

Appendix 1

IPCO
Authorisation & Oversight

PO Box 29105, London
SW1V 1ZU

Mr Oliver Reid
Chief Executive
School Place
Kirkwall
KW15 1NY

16 April 2026

Dear Chief Executive,

Thank you for providing IPCO with your response to the matters identified in my Inspector's letter dated 9 January 2026.

I am satisfied your reply provides your assurance that ongoing compliance with RIP(S)A 2000 and the Investigatory Powers Act 2016 will be maintained. As such, your Council will not require further inspection this year.

I would ask that you ensure the key compliance issues continue to receive the necessary internal governance and oversight through yourself and your Senior Responsible Officer: policy refreshes; annual updates to your Elected Members; ongoing training and awareness raising; internal compliance monitoring by lead managers within their business areas; and the retention, review and destruction (RRD) of any product obtained through the use of covert powers (Records and Product Management in accordance with the Safeguards Chapters of the relevant Codes of Practice).

Your Council will be due its next inspection in 2029, but please do not hesitate to contact my Office if IPCO can be of assistance in the intervening period.

It is, of course, the responsibility of your authority to ensure that any covert activity is conducted in accordance with the legislation. The IPC expects early notification of any Errors in the use of the powers, which will then be investigated fully.

Yours sincerely,

[redacted]

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

**Freedom of Information (Scotland) Act (FOISA)**

*IPCO is not a "public authority" for the purpose of FOISA and therefore falls outside its reach. Public authorities who are subject to these Acts may receive requests for disclosure of our reports. In the first instance the SRO should bring the matter to the IPCO Data Protection Officer (at: info@ipco.org.uk), before making any disclosure.*

**From:** John Coull
**Sent:** 16 April 2026 09:47:26
**To:** Gavin Mitchell
**Subject:** 2026 IPCO Inspection of Orkney Islands Council
**Sensitivity:** Normal
**Attachments:**
20260416 IPCO Inspection conclusion letter Orkney Islands Council.pdf

---


Dear Gavin,

Thank you for submitting the policy documents on behalf of Orkney Islands Council.

I acknowledge the unique circumstances of island life, balancing the limitations and opportunities when addressing public health and crime. I appreciate that RIPSA-enabled tactics aren't always as straightforward to deploy as they are on the mainland. At the same time, the nature of digital investigation, with its hands-off approach, continues to present both ongoing opportunities and risks, and this area requires constant attention.

Overall, I found the documents to be comprehensive, detailed, and compliant with the relevant requirements. Your personal commitment to ensuring everything is up to standard is noted.

I have one suggestion that could further enhance your policy during future reviews. When you next review the Surveillance through Social Media Policy, particularly sections 8.1.1 and 8.1.2, I would encourage you to revisit the language used in light of the IPT rulings. Even when information is publicly accessible online, Article 8 considerations are not automatically negated. This is a complex area, often dependent on the specific platform, the nature of the material, and its intended use. Systematic and targeted monitoring of public content, even when it's available to all, can still amount to directed surveillance.

Our expectation is that directed surveillance may be invoked when activity is focused on an individual, takes place repeatedly over a period, and is likely to result in obtaining private information, irrespective of privacy settings. I encourage you to ensure this important nuance is clearly reflected in the policy wording so that it explicitly addresses these considerations and minimises ambiguity for staff who may be unfamiliar with surveillance legislation.

Thank you once again. The attached letter is for the attention for the Chief Executive and any other parties you consider appropriate. If you have any questions or would like to discuss it further, or require guidance in relation to any future use of RIPSA, please don't hesitate to contact me directly.

Regards,

John

[redacted]
**n Coull**
CHIS and Surveillance Inspector
Investigatory Powers Commissioner's Office

IPCO
Authorisation & Oversight

**Mobile: 07587 421425 | Email: John.Coull@ipco.org.uk**
**Website**: www.ipco.org.uk
**Follow us on:** LinkedIn | X @IPCOffice

**Ensuring lawful compliance through independent authorisation and oversight**
*Information contained in this document is exempt from disclosure under section 23 of the Freedom of Information Act 2000 (FOIA)*

ORKNEY
ISLANDS COUNCIL

# Policy on Covert Surveillance

**Contents**

# 1. Introduction

## 1.1.

In some circumstances, it may be necessary for Council employees where evidence cannot be obtained in any other way, 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 on Human Rights and the Human Rights Act 1998 ("the right to respect for private and family life").

## 1.2.

The Regulation of Investigatory Powers Act (2000) [RIPA], the Regulation of Investigatory Powers (Scotland) Act (2000) [RIP(S)A] and the Investigatory Powers Act 2016 ("the Acts") together provide a legal framework for covert surveillance by public authorities and an independent inspection regime to monitor these activities.

## 1.3.

The Investigatory Powers Act 2016 establishes an Investigatory Powers Commissioner's Office whose remit includes providing comprehensive oversight of the use of powers to which this Policy applies.

## 1.4.

The Investigatory Powers Tribunal, established in terms of RIPA, has jurisdiction to investigate and determine complaints against public authority use of investigatory powers.

## 1.5.

The Chief Executive is the RIPSA Senior Responsible Officer, who has oversight and scrutiny in relation to the RIPSA function and ensures the integrity of the processes in place and acts as the main point of contact with the Investigatory Powers Commissioner. In the Chief Executive's absence, the Head of Corporate Governance will deputise.

## 1.6.

A detailed procedure has been developed for Covert Surveillance ("the Procedure").

# 2. Objective

The objective of this policy is to ensure that all covert surveillance by Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Scottish Government's Code of Practice on Covert Surveillance and Property Interference ("the Code of Practice").

# 3. Scope of the Policy

This Policy applies in all cases where “directed surveillance” is being planned or carried out. Directed surveillance is defined in section 1(2) of the RIP(S) Act as surveillance, which is covert but not intrusive, and undertaken:

## 3.1.

For the purposes of a specific investigation or specific operation.

## 3.2.

In such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation).

## 3.3.

Otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under the RIP(S) Act to be sought for the carrying out of the surveillance. In cases of doubt, the authorisation procedures described below should however be followed.

# 4. Principles of Surveillance

## 4.1.

In planning and carrying out covert surveillance, Council employees shall comply with the following principles.

### 4.1.1.

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 interest of public safety.
- For the purpose of protecting public health.

Employees carrying out surveillance shall not cause damage to any property or harass any person.

### 4.1.2.

Necessity – covert surveillance shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

### 4.1.3.

Effectiveness – planned covert surveillance shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

#### 4.1.4.

Proportionality – the use and extent of covert surveillance shall be as defined in section 6(2) of the RIP(S) Act – that the authorised surveillance is proportionate to what is sought to be achieved by carrying it out.

### 4.2.

Obtaining an authorisation under the Acts will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. The RIP(S)A first requires that the person granting an authorisation is satisfied that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in section 6(3) of the RIP(S) Act for directed surveillance and in section 10(2)(a) of the RIP(S) Act for intrusive surveillance.

### 4.3.

Then, if the activities are necessary, the person granting the authorisation must be satisfied that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activity should be carefully managed to meet the objective in question and must not be arbitrary or unfair.

### 4.4.

Intrusive surveillance – no activity shall be undertaken that comes within the definition of "Intrusive Surveillance", as defined in section 1(3) of the RIP(S) Act as covert surveillance that:

#### 4.4.1.

Is carried out in relation to anything taking place on any residential premises or in any private vehicle.

#### 4.4.2.

Involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

### 4.5.

Collateral intrusion – reasonable steps shall be taken to minimise the acquisition of information that is not directly necessary for the purposes of the investigation or operation being carried out.

### 4.6.

Before authorising surveillance, the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Measures should be

taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.

### 4.7.

Authorisation – all directed surveillance shall be authorised in accordance with the Procedure.

## 5. The Authorisation Process

### 5.1.

The statutory purposes for which covert surveillance authorisations may be issued must reflect the functions of the Council.

### 5.2.

Applications for directed surveillance where knowledge of confidential information is likely to be acquired shall be authorised by a Director.

### 5.3.

Directors should be the designated officer to give the necessary written authorisation for the use or conduct of covert surveillance. In urgent or exceptional circumstances written or oral authorisation might be given by an officer of Chief Officer grade.

### 5.4.

In terms of the Scottish Government`s Code of Practice a written authorisation granted by an authorising officer will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect. Urgent oral authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted or renewed. Further details are contained in the Procedure and Chapter 5 of the Code of Practice.

## 6. Documents

### 6.1.

The Procedure in implementation of this policy uses the following documents:

#### 6.1.1. Covert Surveillance – Written Authorisation

This should be completed by the applicant in all cases not covered by oral authorisation (below). It is effective from the time that approval is given.

#### 6.1.2. Covert Surveillance – Oral Authorisation

This is a record of an oral authorisation, which should be completed by the applicant. It should be used only in cases where the urgency of the situation makes the submission of a written application impractical. The authorising officer should write out a separate authorisation as soon as practical.

### 6.1.3. Covert Surveillance – Renewal of Authorisation

This should be completed by the applicant in all cases where surveillance is required beyond the previously authorised period (including previous renewals) and thereafter signed by the authorising officer.

### 6.1.4. Covert Surveillance – Cancellation

This should be completed by both the applicant and the authorising officer when the authorisation ceases to be either necessary or appropriate.

# 7. Security and Retention of Documents

## 7.1.

Documents created under this procedure are highly confidential and shall be treated as such. Services must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of covert surveillance. Authorising officers must ensure compliance with the requirements of data protection legislation, the Procedure for Authorisation of Covert Surveillance, Chapter 8 of the Scottish Government's Code of Practice on Covert Surveillance and Property Interference and the Council's RIPSA Data Safeguards Compliance Process.

## 7.2.

The Head of Corporate Governance shall maintain a register of current and past authorisations. Applicant officers shall ensure that sufficient information is provided to keep this up to date.

# 8. Central Record of all Authorisations

## 8.1.

A centrally retrievable record of all authorisations should be held by the Head of Corporate Governance and be regularly updated whenever an authorisation is granted, renewed or cancelled. The record should be made available to the relevant Inspector from the Investigatory Powers Commissioner's Office, upon request. These records should be retained for a period of five years from the ending of the authorisation and should contain the following information:

- 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 is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer.
- Whether the investigation or operations is likely to result in obtaining confidential information as defined in this code of practice.
- The date the authorisation was cancelled.

## 8.2.

In all cases, Services should maintain for a period of three years the following documentation which need not form part of the centrally retrievable record:

- A copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer.
- A record of the period over which the surveillance has taken place.
- A record of the result of each review of the authorisation.
- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested.
- The date and time when any instruction was given by the authorising officer.

# Document control Sheet

### Review / Approval History

| Date | Name | Position | Version Approved |
|---|---|---|---|
| 1 May 2018 | Gavin Mitchell | Head of Legal Services | V1.2– approved at General Meeting of the Council |
| 11 May 2020 | Gavin Mitchell | Head of Legal Services | V1.3 |
| 5 May 2021 | Gavin Mitchell | Head of Legal Services | V1.3 |
| 9 October 2023 | Gavin Mitchell | Head of Legal and Governance | V1.4 |
| 7 October 2025 | Gavin Mitchell | Head of Corporate Governance | V1.5 |

### Change Record Table

| Date | Author | Version | Status | Reason |
|---|---|---|---|---|
| 11 May 2020 | Gavin Mitchell | V1.3 | Final | Reflect observations contained in IPC Inspection Report |
| 9 October 2023 | Gavin Mitchell | V1.4 | Final | Reflect observations contained in P&R Committee report on 19 September 2023 and subsequently ratified by Full Council on 3 October 2023. |
| 7 October 2025 | Gavin Mitchell | V1.5 | Final | Reflect observations contained in P&R Committee report on 23 September 2025 and subsequently ratified by Full Council on 7 October 2025. |

ORKNEY
ISLANDS COUNCIL

# Procedure for Authorisation of Covert Surveillance

**Contents**

# 1. Foreword

## 1.1.

The use of surveillance to provide information is a valuable resource for the protection of the public and the maintenance of law and order. In order that local authorities and law enforcement agencies are able to discharge their responsibilities, use is made of unaided surveillance and surveillance devices. Where this surveillance is covert i.e. the subject of the surveillance is unaware that it is taking place, then it must be authorised to ensure that it is lawful. CCTV systems in the main will not be subject to this procedure as they are 'overt' forms of surveillance. However where CCTV is used as part of a pre-planned operation of surveillance then authorisation should be obtained. This includes circumstances where such use is sought by the Council or by a third party such as the Police. For the use of CCTV for covert surveillance, officers should refer to paragraph 10 of the Council's CCTV Code of Practice.

## 1.2.

A legal framework ensures that the use of surveillance is subject to an authorisation, review and cancellation procedure.

# 2. Implications of this Procedure

## 2.1.

In some circumstances, it may be necessary for Orkney Islands Council employees, in the course of their duties, to make observations of a person or person(s) in a covert manner, i.e. without that person's knowledge. By their nature, actions of this sort may constitute an interference with that person's right to privacy and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 ('the right to respect for private and family life').

## 2.2.

The Regulation of Investigatory Powers Act (2000) [RIPA], the Regulation of Investigatory Powers (Scotland) Act (2000) [RIP(S) A] and the Investigatory Powers Act 2016 ('the Acts') together provide a legal framework for covert surveillance activities by public authorities (including local authorities) and an independent inspection regime to monitor these activities.

## 2.3.

Whilst the Acts do not impose a requirement for local authorities to seek or obtain an authorisation, where one is available, Orkney Islands Council employees will adhere to the authorisation procedure before conducting any covert surveillance.

## 2.4.

Employees of Orkney Islands Council will not carry out intrusive surveillance within the meaning of the Regulation of Investigatory Powers (Scotland) Act 2000. This is surveillance of anything taking place on residential premises or in a private vehicle

that involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device capable of providing information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the house or vehicle.

### 2.5.

A number of practical examples of the use of directed surveillance are contained in sections 3 and 4 of the Scottish Government's Code of Practice on Covert Surveillance and Property Interference.

## 3. Objective

### 3.1.

The objective of this procedure is to ensure that all work involving directed surveillance by Orkney Islands Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Regulation of Investigatory Powers (Scotland) Act 2000 and the Scottish Government's Code of Practice on Covert Surveillance and Property Interference ("the Code of Practice").

### 3.2.

Definitions:

#### 3.2.1.

Covert surveillance means surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is taking place.

#### 3.2.2.

Authorising officer is the person who is entitled to give an authorisation for directed surveillance in accordance with section 6 of the Regulation of Investigatory Powers (Scotland) Act 2000.

#### 3.2.3.

Private Information includes information about a person relating to their private or family life.

#### 3.2.4.

Residential premises means any premises occupied or used, however temporarily, for residential purposes or otherwise as living accommodation.

#### 3.2.5.

Private vehicle means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. This does not include a person whose right to use the vehicle derives only from their having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey. A vehicle includes any vessel, aircraft or hovercraft.

# 4. Scope of the Procedure

## 4.1.

This procedure applies in all cases where 'direct surveillance' is being planned or carried out. Direct surveillance is defined in the Code of Practice as surveillance undertaken "for the purposes of a specific investigation or operation" and "in such a manner as is likely to result in the obtaining of private information about a person".

## 4.2.

The procedure does not apply to:

- Ad-hoc covert observations that do not involve the systematic surveillance of specific person(s).
- Observations that are not carried out covertly.
- Unplanned observations made as an immediate response to events.

## 4.3.

Particular attention should be made to Social Media Networking Sites. A separate policy is in place in connection with surveillance through social media and should be consulted as necessary.

## 4.4.

In cases of doubt, the authorisation procedures described below should be followed.

# 5. Principles of Surveillance

In planning and carrying out covert surveillance, Orkney Islands Council employees shall comply with the following principles.

## 5.1. Lawful purposes

### 5.1.1.

Directed surveillance shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in the Acts) namely:

- 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.

### 5.1.2.

Employees carrying out surveillance shall not interfere with any property or harass any person.

## 5.2. Confidential material

### 5.2.1.

Particular care should be taken with applications where a significant risk of acquiring confidential material has been identified.

**5.2.2.**

Confidential material consists of:

- Matters subject to legal privilege (for example between professional legal advisor and client). In terms of the Regulation of Investigatory Powers (Modification of the Authorisation Provisions: Legal Consultations) (Scotland) Order 2015, directed surveillance carried out on premises in respect of matters subject to legal privilege is to be treated as intrusive surveillance and can only be carried out by the police.
- Confidential personal information (for example relating to a person's physical or mental health).
- Confidential journalistic material.

# 6. The Authorisation Process

## 6.1.

Applications for directed surveillance will be authorised by a Director. In urgent or exceptional circumstances written or oral authorisation might be given by an officer of Chief Officer grade who has not been designated which should as soon as practicable be followed up by a written authorisation from the relevant official.

## 6.2.

Authorising officers within the meaning of this procedure should avoid authorising their own activities wherever possible and only do so in exceptional circumstances.

## 6.3.

All applications for directed surveillance authorisations will be made on the appropriate application form. The applicant in all cases should complete this. In urgent cases the authorising officer may give an oral authorisation. A statement that the authorising officer has expressly granted the authorisation should be recorded on the form or, if that is not possible, in the applicant's notebook or diary. This should be done by the person to whom the authorising officer spoke (normally the applicant) but should later be endorsed by the authorising officer. The authorising officer should write out a separate authorisation as soon as practical.

## 6.4.

All applications for directed surveillance renewals will be made on the appropriate form. The applicant in all cases should complete this where the surveillance requires to continue beyond the previously authorised period (including previous renewals). The renewal of the authorisation should be considered and signed by the authorising officer.

## 6.5.

Where authorisation ceases to be either necessary or appropriate the authorising officer will cancel an authorisation using the appropriate form submitted by the applicant.

## 6.6.

Forms, codes of practice and supplementary material are available on the Council's Intranet.

## 6.7.

Any person giving an authorisation for the use of directed surveillance must be satisfied that:

- Account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation ('collateral intrusion'). Measures must be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion.
- The authorisation is necessary (see below).
- The authorised surveillance is proportionate (see below).
- In particular when Environmental Health Investigators deploy DAT noise level monitors to assist in any enforcement action in relation to noisy neighbour complaints. These cases should be reviewed on a case by case basis and if necessary the appropriate authorisation sought.
- In relation to aerial surveillance, using, for example, drones, the same considerations should be made to determine whether a directed surveillance authorisation is appropriate. In considering whether the surveillance should be regarded as covert, account should be taken of the reduced visibility of a craft or device at altitude.

## 6.8. Necessity

Surveillance operations shall only be undertaken where an authorisation is necessary on grounds falling within S.6(3) of RIP(S)A if it is necessary (a) for the purpose of preventing or detecting crime or of preventing disorder; (b) in the interests of public safety; or (c) for the purpose of protecting public health.

## 6.9. Effectiveness

Surveillance operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

## 6.10. Proportionality

The use of surveillance shall be proportionate in terms of S6(2)(b) of RIP(S)A to what is sought to be achieved by carrying it out. Further there must be no other reasonable and effective way of achieving the desired objective(s).

A potential model answer would make clear that the following elements of proportionality had been fully considered:

- balancing the size and scope of the operation against the gravity and extent of the perceived mischief.
- explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others.
- that the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result.

- providing evidence of other methods considered and why they were not implemented.

## 6.11. Authorisation

**6.11.1.**

All directed surveillance shall be authorised in accordance with this procedure.

The authorising officer must take into account the following issues when considering an application:

- who is to conduct the operation.
- what is being proposed.
- where and when the proposed operation will take place.
- whether it is necessary and proportionate.

**6.11.2.**

Underlying all of these considerations is the requirement for the authorising officer to be satisfied that the terms of the legislation and relevant guidance are met.

**6.11.3.**

The case for the authorisation should be presented in the application in a fair and balanced way. In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation.

**6.11.4.**

The authorising officer should clearly complete the “Authorising Officer’s Statement” on the application form, preferably in their own hand, and articulate in their own words what activity they are authorising.

**The Authorising Officer must state explicitly what is being authorised.**

**6.11.5.**

The Authorising Officer must describe and specify what they are granting. This may or may not be the same as requested by the applicant. For the benefit of those operating under the terms of an authorisation, or any person who may subsequently review or inspect an authorisation, it is essential to produce, with clarity, a description of that which is being authorised (i.e. who, what, where, when and how). The Authorising Officer should as a matter of routine state explicitly and in their own words what is being authorised, and against which subjects, property or location.

**6.11.6.**

Mere reference to the terms of the application is inadequate. The Authorising Officer should specify the details of how and why they consider the application to be both necessary and proportionate.

**Authorisation different from application.**

**6.11.7.**

If an application fails to include an element in the proposed activity which in the opinion of the Authorising Officer should have been included (for example, the return of something to the place from which it is to be taken for some specified activity), or which is subsequently requested orally by the applicant, it may be included in the authorisation; if so, a note should be added explaining why. Conversely, if an Authorising Officer does not authorise all that was requested, a note should be added explaining why. This requirement applies equally to intrusive surveillance, property interference, directed surveillance and CHIS authorisations.

**The Senior Responsible Officer should avoid granting authorisations.**

**6.11.8.**

The role of the Senior Responsible Officer is to oversee the competence of Authorising Officers and the processes in use in their public authority. Whilst legislation does not preclude their use as an Authorising Officer, it is unlikely that they would be regarded as objective if they oversee their own authorisations.

**6.11.9.**

Applications for covert surveillance that may result in the acquisition of knowledge of matters subject to legal privilege within the meaning given in paragraph 1.1 of the Code of Practice should state whether the covert surveillance is likely or intending to obtain knowledge of matters subject to legal privilege. Where covert surveillance is likely or intended to result in the acquisition of knowledge of matters subject to legal privilege, an authorisation shall only be granted or approved if the Authorising Officer is satisfied that there are exceptional and compelling circumstances that make the authorisation necessary.

**6.11.10.**

Where the surveillance is not intended to result in the acquisition of knowledge of matters subject to legal privilege, such exceptional and compelling circumstances may arise in the interests of preventing or detecting serious crime.

**6.11.11.**

Where the surveillance is intended to result in the acquisition of knowledge of matters subject to legal privilege, such circumstances will arise only in a very restricted range of cases, such as where there is a threat to life or limb and the surveillance is reasonably regarded as likely to yield intelligence necessary to counter the threat.

# 7. Time Periods – Authorisations

## 7.1.

Urgent oral authorisations granted by a person who is entitled to act only in urgent cases unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted or renewed.

### 7.2.

In terms of the Scottish Government's Code of Practice a written authorisation granted by an Authorising Officer will cease to have effect (unless renewed) at the end of a period of three months beginning with the day on which it took effect.

## 8. Time Periods – Renewals

### 8.1.

If at any time before an authorisation would cease to have effect, the Authorising Officer considers it necessary and proportionate for the authorisation to continue for the purpose for which it was given, the authorisation may be renewed in writing for a further period of three months. Renewals may also be granted orally in urgent cases and last for a period of 72 hours. Applications should only be made shortly before the authorisation is due to expire.

### 8.2.

Any person entitled to authorise may renew authorisations. They may be renewed more than once, provided they continue to meet the criteria for authorisation.

## 9. Review

### 9.1.

The Authorising Officer shall keep all authorisations under constant review and an authorisation will be cancelled immediately the requirement for surveillance ceases. The Authorising Officer should set review dates and ensure that all reviews are carried out with the review period tailored to meet the particular requirements of the investigation. Details of the review and the decision reached shall be noted on the Review Form.

### 9.2.

During a review, the Authorising Officer who granted or last renewed the authorisation may amend specific aspects of the authorisation, for example, to cease directed surveillance against one of a number of named subjects or to discontinue the use of a particular tactic.

### 9.3.

Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or particularly sensitive information is likely to be obtained. At the point when the Council is considering applying for an authorisation, it must have regard to whether the level of protection to be applied in relation to information obtained under the warrant or authorisation is higher because of the particular sensitivity of that information.

### 9.4.

In each case, unless specified by the Investigatory Powers Commissioner's Office, the frequency of reviews should be determined by the Council. This should be as frequently as is considered necessary and proportionate.

### 9.5.

In the event that there are any significant and substantive changes to the nature of the operation during the currency of the authorisation, the Council should consider whether it is necessary to apply for a new authorisation.

## 10. Cancellation

### 10.1.

Those acting under an authorisation must keep their authorisations under review and notify the Authorising Officer if they consider that the authorisation is no longer necessary or proportionate, and so should therefore be cancelled.

### 10.2.

The Authorising Officer and the applicant must cancel an authorisation if they are satisfied that the directed surveillance no longer satisfies the criteria for authorisation.

## 11. Record Keeping

Each Service or discrete location within Services must maintain a record of all applications for authorisation (including refusals), renewals, reviews and cancellations. A centrally retrievable record of all authorisations will be held by the Head of Corporate Governance and be regularly updated whenever an authorisation is granted, renewed or cancelled. An application for authorisation cannot proceed until a unique reference number (URN) has been issued by the Head of Corporate Governance and the Head of Corporate Governance must have sight of each and every application. The central register should be kept up-to-date at all times. The record should be made available to the relevant Inspector from the Investigatory Powers Commissioner's Office, upon request. These records should be retained for a period of at least five years. Section 8 of Orkney Islands Council's Policy on Covert Surveillance contains further details.

## 12. Security and Retention of Documents

### 12.1.

Documents created under this procedure are highly confidential and shall be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of data protection legislation and Chapter 8 of the Scottish Government's Code of Practice on Covert Surveillance and Property Interference and the Council's RIPSA Data Safeguards Compliance Process.

### 12.2.

Dissemination or copying of material must be limited to the minimum necessary for authorised purposes. The purposes are authorised if the material:

- Is, or is likely to become, necessary for any of the statutory purposes set out in RIPSA in relation to covert surveillance or property interference;
- Is necessary for facilitating the carrying out of the functions of public authorities under RIPSA;
- Is necessary for facilitating the carrying out of any functions of the Investigatory Powers Commission or the Investigatory Powers Tribunal;
- Is necessary for the purposes of legal proceedings; or
- Is necessary for the performance of the functions of any person by or under any enactment.

### 12.3.

The Head of Corporate Governance will maintain the Central Register of Authorisations. Authorising Officers shall notify the Head of Corporate Governance of the grant, renewal or cancellation of any authorisations and the name of the Applicant Officer within one working day to ensure the accuracy of the Central Register.

### 12.4.

The Authorising Officer shall retain the original Authorisation and Renewal Forms until cancelled. On cancellation, the original Application, Renewal and Cancellation forms shall be forwarded to the Head of Corporate Governance with the Authorising Officer retaining a copy.

### 12.5.

The Authorising Officer shall retain the copy forms for a period of three years after cancellation. The Head of Corporate Governance will retain the original forms for a period of five years after cancellation. In both cases these will not be destroyed without the authority of the Authorising Officer if practicable.

## 13. Oversight

The Investigatory Powers Act 2016 establishes an Investigatory Powers Commissioner's Office to provide comprehensive oversight of the use of the powers to which this Procedure applies. This oversight includes inspection visits by Inspectors appointed by the Investigatory Powers Commissioner.

## 14. Complaints

The Investigatory Powers Tribunal has jurisdiction to investigate and determine complaints against public authority use of investigatory powers. Any complaints in respect of the use by the Council of its powers described in this Procedure should be directed to the Investigatory Powers Tribunal. Full details of how to present a complaint are available on the Tribunal's website – https://investigatorypowerstribunal.org.uk/.

# Document control Sheet

### Review / Approval History

| Date | Name | Position | Version Approved |
|---|---|---|---|
| 1 May 2018 | Gavin Mitchell | Head of Legal Services | V1.2– approved at General Meeting of the Council |
| 11 May 2020 | Gavin Mitchell | Head of Legal Services | V1.3 |
| 5 May 2021 | Gavin Mitchell | Head of Legal Services | V1.3 |
| 9 October 2023 | Gavin Mitchell | Head of Legal and Governance | V1.4 |
| 7 October 2025 | Gavin Mitchell | Head of Corporate Governance | V1.5 |

### Change Record Table

| Date | Author | Version | Status | Reason |
|---|---|---|---|---|
| 11 May 2020 | Gavin Mitchell | V1.3 | Final | Reflect observations contained in IPC Inspection Report |
| 9 October 2023 | Gavin Mitchell | V1.4 | Final | Reflect observations contained in P&R Committee report on 19 September 2023 and subsequently ratified by Full Council on 3 October 2023. |
| 7 October 2025 | Gavin Mitchell | V1.5 | Final | Reflect observations contained in P&R Committee report on 23 September 2025 and subsequently ratified by Full Council on 7 October 2025. |

ORKNEY
ISLANDS COUNCIL

# Policy on Use of Covert Human Intelligence Sources

.

## Contents

# 1. Introduction

## 1.1.

In some circumstances, it may be necessary for Orkney Islands Council employees where evidence cannot be obtained in any other way, in the course of their duties, to make use of informants and to conduct 'undercover' operations in a covert manner, i.e. without a person's knowledge. By their nature, actions of this sort may constitute an interference with that person's right to privacy and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 ("the right to respect for private and family life").

## 1.2.

The Regulation of Investigatory Powers Act (2000) [RIPA], the Regulation of Investigatory Powers (Scotland) Act (2000) [RIP(S)A] and the Investigatory Powers Act 2016 ("the Acts") together provide a legal framework for use of Covert Human Intelligence Sources by public authorities and an independent inspection regime to monitor these activities.

## 1.3.

The Investigatory Powers Act 2016 establishes an Investigatory Powers Commissioner's Office whose remit includes providing comprehensive oversight of the use of powers to which this Policy applies.

## 1.4.

The Investigatory Powers Tribunal, established in terms of RIPA, has jurisdiction to investigate and determine complaints against public authority use of investigatory powers.

## 1.5.

The Chief Executive is the RIPSA Senior Responsible Officer, who has oversight and scrutiny in relation to the RIPSA function and ensures the integrity of the processes in place and acts as the main point of contact with the Investigatory Powers Commission. In the Chief Executive's absence, the Head of Corporate Governance will deputise.

## 1.6.

A detailed procedure has been developed for Covert Human Intelligence Sources ("the Procedure").

# 2. Objective

The objective of this Policy is to ensure that all use or conduct of a source by Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Scottish Government's Covert human intelligence sources: code of practice ("the Code of Practice").

# 3. Scope of the Policy

## 3.1.

This Policy applies in all cases where the use of an undercover officer or source is being planned or carried out. All Officers involved should be suitably trained and experienced.

## 3.2.

This Policy does not apply to covert test purchase transactions under existing statutory powers where the officers involved do not establish a personal or other relationship for the purposes stated. As an example the purchase of music CD for subsequent expert examination would not require authorisation but where the intention is to ascertain from the seller where he/she buys suspected fakes, when he/she takes delivery etc. then authorisation should be sought beforehand; or tasks given to persons (whether that person is an employee of the Council or not) to ascertain purely factual information (for example the location of cigarette vending machines in licensed premises).

## 3.3.

In terms of Section 1(7) of RIPSA a person is a covert human intelligence source if the person:

1. Establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating the doing of anything falling within paragraph 2 or 3 below.

2. Covertly uses such a relationship to obtain information or to provide access to any information to another person.

3. Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

# 4. Principles of the Use and Conduct of a Source

## 4.1.

In planning and carrying out the use of covert human intelligence sources, Council employees shall comply with the following principles.

### 4.1.1.

Lawful purposes – the use and conduct of a source 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:

1. For the purpose of preventing or detecting crime or the prevention of disorder.

2. In the interest of public safety.

3. For the purpose of protecting public health.

Employees carrying out source work or using sources must be aware that a source has no licence to commit crime.

**4.1.2.**

Necessity – An authorisation for the use of a Covert Human Intelligence Source is necessary on grounds falling within section 7 (3) of RIP(S)A if it is necessary (a) for the purpose of preventing or detecting crime or of preventing disorder; (b) in the interests of public safety; or (c) for the purpose of protecting public health.

**4.1.3.**

Effectiveness – planned undercover operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

**4.1.4.**

Proportionality – the use and extent of a source shall be as defined in section 6(2) of the RIP(S)A – that the authorised use and conduct of a source is proportionate to what is sought to be achieved by carrying it out.

## 4.2.

Obtaining an authorisation under RIP(S)A will only ensure that the authorised use or conduct of a source is a justifiable interference with an individual's Article 8 rights it if is necessary and proportionate for the source to be used. RIP(S)A first requires that the person granting an authorisation is satisfied that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in section 7(3) of RIP(S)A.

## 4.3.

If the use of the source is necessary, the person granting the authorisation must be satisfied that the use of a source is proportionate to what is sought to be achieved by the conduct and use of that source. This involves balancing the intrusiveness of the use of the source on the target and others who might be affected by it against the need for the source to be used in operational terms. The use of a source will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. The use of a source should be carefully managed to meet the objective in question and sources must not be used in an arbitrary or unfair way.

## 4.4.

Collateral intrusion – reasonable steps shall be taken to minimise the acquisition of information that is not directly necessary for the purposes of the investigation or operation being carried out.

## 4.5.

Before authorising the use or conduct of a source, the Authorising Officer should take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the operation or investigation (collateral intrusion).

Measures should be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation or investigation.

### 4.6.

Authorisation – all use and conduct of Covert Human Intelligence Sources shall be authorised in accordance with the Procedure. Additionally, the Authorising Officer must make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation and satisfactory arrangements exist for the management of the source.

## 5. The Authorisation Process

### 5.1.

Applications for use of a Covert Human Intelligence Source will be authorised by a Director.

### 5.2.

A Director should be a designated officer to give the necessary written authorisation for the use or conduct of a Covert Human Intelligence Source. In urgent or exceptional circumstances written or oral authorisation might be given by an officer of Chief Officer grade which should as soon as practicable be followed up by a written authorisation from the relevant official.

### 5.3.

In terms of the Scottish Government's Code of Practice a written authorisation granted by an Authorising Officer will cease to have effect (unless renewed) at the end of a period of 12 months beginning with the day on which it took effect. Urgent oral authorisations granted by a person who is entitled to act only in urgent cases will unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted or renewed. Further details are contained in the Procedure. Particular special rules apply to the use of vulnerable individuals or juvenile sources. Additional guidance is contained in Chapter 5 of the Code of Practice.

## 6. Documents

### 6.1.

The Procedure in implementation of this Policy uses the following documents:

**1. Use or conduct of a covert human intelligence source – Written Authorisation**

This should be completed by the applicant in all cases not covered by oral authorisation (below). It is effective from the time that approval is given.

### 2. Use or conduct of a covert human intelligence source – Oral Authorisation

This is a record of an oral authorisation, which should be completed by the applicant. It should be used only in cases where the urgency of the situation makes the submission of a written application impractical. The Authorising Officer should write out a separate authorisation as soon as practical.

### 3. Use or conduct of a covert human intelligence source – Renewal of Authorisation

This should be completed by the applicant in all cases where surveillance is required beyond the previously authorised period (including previous renewals) and thereafter signed by the Authorising Officer.

### 4. Use or conduct of a covert human intelligence source – Cancellation

This should be completed by both the applicant and the Authorising Officer when the authorisation ceases to be either necessary or appropriate.

# 7. Security and Retention of Documents

## 7.1.

Documents created under this procedure are highly confidential and shall be treated as such. Services must ensure that arrangements are in place for the handling, storage and destruction of material obtained through the use of a covert human intelligence source. Authorising Officers must ensure compliance with the requirements of data protection legislation, the Procedure for Authorisation of the use of Covert Human Intelligence Sources, Chapter 7 of the Scottish Government's Code of Practice on Covert Human Intelligence Sources and the Council's RIPSA Data Safeguards Compliance Process.

## 7.2.

The Head of Corporate Governance shall maintain a register of current and past authorisations. Applicant officers shall ensure that sufficient information is provided to keep this up to date.

# 8. Central Record of all Authorisations

## 8.1.

A centrally retrievable record of all authorisations should be held by the Head of Corporate Governance and be regularly updated whenever an authorisation is granted, renewed or cancelled. The record should be made available to the relevant Inspector from the Investigatory Powers Commissioner's Office, upon request. These records should be retained for a period of five years from the ending of the authorisation and should contain the following information:

- 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 is renewed, when it was renewed and who authorised the renewal, including the name and rank/grade of the authorising officer.
- Whether the investigation or operations is likely to result in obtaining confidential information as defined in this code of practice.
- The date the authorisation was cancelled.

## 8.2.

In all cases, Services should maintain for a period of three years the following documentation which need not form part of the centrally retrievable record:

- A copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the approval given by the authorising officer.
- A record of the period over which the activities of the source has taken place.
- A record of the result of each review of the authorisation; the results of which should be recorded in the central record.
- A copy of any renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested.
- The date and time when any instruction was given by the authorising officer.

# Document control Sheet

### Review / Approval History

| Date | Name | Position | Version Approved |
|---|---|---|---|
| 1 May 2018 | Gavin Mitchell | Head of Legal Services | V1.2– approved at General Meeting of the Council |
| 11 May 2020 | Gavin Mitchell | Head of Legal Services | V1.3 |
| 5 May 2021 | Gavin Mitchell | Head of Legal Services | V1.3 |
| 9 October 2023 | Gavin Mitchell | Head of Legal and Governance | V1.4 |
| 7 October 2025 | Gavin Mitchell | Head of Corporate Governance | V1.5 |

### Change Record Table

| Date | Author | Version | Status | Reason |
|---|---|---|---|---|
| 11 May 2020 | Gavin Mitchell | V1.3 | Final | Reflect observations contained in IPC Inspection Report |
| 9 October 2023 | Gavin Mitchell | V1.4 | Final | Reflect observations contained in P&R Committee Report on 19 September 2023 and subsequently ratified by Full Council on 3 October 2023. |
| 7 October 2025 | Gavin Mitchell | V1.5 | Final | Reflect observations contained in P&R Committee Report on 23 September 2025 and subsequently ratified by Full Council on 7 October 2025. |

ORKNEY
ISLANDS COUNCIL

# Procedure for Authorisation of the use of Covert Human Intelligence Sources

## Contents

# 1. Foreword

## 1.1.

The use of human beings to provide information ('informants') is a valuable resource for the protection of the public and the maintenance of law and order. In order that local authorities and law enforcement agencies are able to discharge their responsibilities, use is made of 'undercover' officers and informants. These are referred to as 'covert human intelligence sources' or 'sources' and the area of work of undercover officers and informants to whom this procedure applies will be referred to as 'source work'.

## 1.2.

A legal framework ensures that the use, deployment, duration and effectiveness of sources is subject to an authorisation, review and cancellation procedure.

# 2. Implications of this Procedure

## 2.1.

In some circumstances, it may be necessary for Orkney Islands Council employees, in the course of their duties, to make use of informants and to conduct 'undercover' operations in a covert manner, i.e. without a person's knowledge. By their nature, actions of this sort may constitute an interference with that person's right to privacy and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 ('the right to respect for private and family life').

## 2.2.

The Regulation of Investigatory Powers Act (2000) [RIPA] and the Regulation of Investigatory Powers (Scotland) Act (2000) [RIP(S)A] and the Investigatory Powers Act 2016 ('the Acts') together provide a legal framework for covert surveillance activities by public authorities (including local authorities) and an independent inspection regime to monitor these activities.

## 2.3.

Whilst the Acts do not impose a requirement for local authorities to seek or obtain an authorisation, where one is available Orkney Islands Council employees will adhere to the authorisation procedure before using a source or allowing or conducting an undercover operation.

## 2.4.

Employees of Orkney Islands Council will not carry out intrusive surveillance within the meaning of RIPSA nor will they authorise any person for any covert human intelligence source activity as an opportunity to install any surveillance equipment into residential premises or private vehicle.

### 2.5.

A number of practical examples of the use of covert human intelligence sources are contained in sections 2, 3 and 4 of the Scottish Government's Code of Practice on Covert Human Intelligence Sources.

## 3. Objective

### 3.1.

The objective of this procedure is to ensure that all work involving the use or conduct of a source by Orkney Islands Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Regulation of Investigatory Powers (Scotland) Act 2000 and the Scottish Government's Code of Practice on the Use of Covert Human Intelligence Sources ("the Code of Practice").

### 3.2. Definitions

#### 3.2.1.

Covert human intelligence source means a person who establishes or maintains a personal relationship with another person for the covert purpose of facilitating anything that:

1. Covertly uses such a relationship to obtain information or to provide information or to provide access to information to another person; or

2. Covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose.

#### 3.2.2.

Directed surveillance is defined in the Code of Practice as surveillance undertaken "for the purposes of a specific investigation or operation" and "in such a manner as is likely to result in the obtaining of private information about a person".

#### 3.2.3.

Authorising Officer is the person who is entitled to give an authorisation for use and conduct of a Covert Human Intelligence Source in accordance with section 7 of the Regulation of Investigatory Powers (Scotland) Act 2000.

#### 3.2.4.

Handler means the person referred to in section 7(6) of the Regulation of Investigatory Powers (Scotland) Act 2000 holding an office or position within the local authority and who will have day to day responsibility for:

- Dealing with the source on behalf of the local authority.
- Directing the day to day activities of the source.

- Recording the information supplied by the source.
- Monitoring the source's security and welfare.

**3.2.5.**

Controller means the person/the designated managerial officer within the local authority referred to in section 7(6)(b) of the Regulation of Investigatory Powers (Scotland) Act 2000, responsible for the general oversight of the use of the source.

**3.2.6.**

The conduct of a source is action of that source, falling within the terms of the Regulation of Investigatory Powers (Scotland) Act 2000, or action incidental to it.

**3.2.7.**

The use of a source is any action to induce, ask or assist a person to engage in the conduct of a source or to obtain information by means of an action of the source.

**3.2.8.**

Private information includes information about a person relating to their private or family life.

**3.2.9.**

Residential premises means any premises occupied or used, however temporarily for residential purposes or otherwise as living accommodation.

**3.2.10.**

Private vehicle means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. This does not include a person whose right to use the vehicle derives only from their having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey. A vehicle includes any vessel, aircraft or hovercraft.

# 4. Scope of the Procedure

## 4.1.

This procedure applies in all cases where the use of an undercover officer or source is being planned or carried out.

## 4.2.

The procedure does not apply to:

- Covert test purchase transactions under existing statutory powers where the officers involved do not establish a personal or other relationship for the purposes stated (see definition of a covert human intelligence source). As an example, the purchase of a music CD for subsequent expert examination would not require authorisation but where the intention is to ascertain from the seller where they buy suspected fakes, when they take delivery etc. then authorisation should be sought beforehand.

- Tasks given to persons (whether that person is an employee of the Council or not) to ascertain purely factual information (for example the location of cigarette vending machines in licensed premises).

- Particular attention should be made to Social Media Networking Sites. A separate policy is in place in connection with surveillance through social media and should be consulted as necessary. In cases of doubt, the authorisation procedures described below should be followed.

# 5. Principles of Use or Conduct of Covert Human Intelligence Source

In planning and carrying out the source work, Orkney Islands Council employees shall comply with the following principles.

## 5.1. Lawful purposes

Source work shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in the Acts) namely:

- 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.

Employees carrying out source work or using sources must be aware that a source has no licence to commit crime. Any source that acts beyond the acceptable limits of case law in regard to this principle risks prosecution.

It may be necessary to deploy directed surveillance against a potential source as part of the process of assessing their suitability for recruitment, or in planning how best to make the approach to them. An authorisation under this procedure authorising an officer to establish a covert relationship with a potential source could be combined with a directed surveillance authorisation so that both the officer and potential source could be followed.

## 5.2. Confidential material

### 5.2.1.

Particular care should be taken with applications where a significant risk of acquiring confidential material has been identified.

### 5.2.2.

Confidential material consists of:

- Matters subject to legal privilege (for example between professional legal advisor and client); special rules apply in relation to directed surveillance carried out on premises where legal consultations are taking place and are referred to in the Procedure for Authorisation of Covert Surveillance.

- Confidential personal information (for example relating to a person's physical or mental health).

- Confidential journalistic material.

## 5.3. Vulnerable individuals

### 5.3.1.

Vulnerable individuals, such as a person aged 16 or over whose ability to protect him/herself from violence, abuse or neglect is significantly impaired through physical or mental disability or illness, through old age or otherwise, will only be authorised to act as a source in the most exceptional circumstances.

### 5.3.2.

Special safeguards also apply to the use or conduct of juvenile sources, that is, those under the age of 18 years. The use or conduct of any source under 16 years of age living with their parents cannot be authorised to give information about their parents.

### 5.3.3.

Subject to the above, juvenile sources can give information about members of their immediate family in exceptional cases. A parent, guardian or other 'appropriate adult' should be present at meetings with the juvenile source under the age of 16 years.

### 5.3.4.

An authorisation for the conduct or use of a source may not be granted or renewed in any case where the source is under the age of 18 at the time of the grant or renewal, unless:

- A person holding an office, rank or position with the relevant investigating authority has made and, in the case of a renewal, updated a risk assessment sufficient to demonstrate that:
  - The nature and magnitude of any risk of physical injury to the source arising in the course of, or as a result of, carrying out the conduct described in the authorisation have been identified and evaluated.
  - The nature and magnitude of any risk of psychological distress to the source arising in the course of carrying out the conduct described in the authorisation have been identified and evaluated.

- The person granting or renewing the authorisation has considered the risk assessment and is satisfied that any risks identified in it are justified and, if they are, that they have been properly explained to and understood by the source.

- The person granting or renewing the authorisation knows whether the relationship to which the conduct or use would relate is between the source and a relative, guardian or person who has for the time being assumed responsibility for the source's welfare, and, if it is, has given particular consideration to whether the authorisation is justified in the light of that fact.

# 6. The Authorisation Process

## 6.1.

Applications for the use or conduct of a source will be authorised by a Director, who will give the necessary written authorisation for the use or conduct of the Covert Human Intelligence Source. In urgent or exceptional circumstances written or oral authorisation might be given by an officer of Chief Officer grade who has not been designated which should as soon as practicable be followed up by a written authorisation from the relevant official.

## 6.2.

Authorising Officers should ensure that arrangements are in place for the proper oversight and management of sources, including appointing individual officers as defined in section 7(6)(a) and (b) of RIP(S)A for each source as handler and controller. All Officers involved should be suitably trained and experienced.

## 6.3.

Authorising Officers should not be responsible for authorising their own activities, for example, those in which they, themselves, are to act as the Covert Human Intelligence Source or the handler of the Covert Human Intelligence Source. Furthermore, Authorising Officers should, where possible, be independent of the investigation. It is recognised that this is not always possible, especially in the cases of small organisations. However, where possible, clear separation should be maintained between those responsible for the investigation and those managing the Covert Human Intelligence Source to ensure that the safety and welfare of the Source are always given due consideration.

## 6.4.

All applications for covert human intelligence source authorisations will be made on the appropriate form. The applicant in all cases should complete this. In urgent cases an oral authorisation may be given by the Authorising Officer. A statement that the Authorising Officer has expressly granted the authorisation should be recorded on the form or, if that is not possible, in the applicant's notebook or diary. This should be done by the person to whom the Authorising Officer spoke (normally the applicant) but should later be endorsed by the Authorising Officer. The Authorising Officer should write out a separate authorisation as soon as practical.

## 6.5.

The case for the authorisation should be presented in the application in a fair and balanced way.  In particular, all reasonable efforts should be made to take account of information which supports or weakens the case for the authorisation.

## 6.6.

All applications for covert human intelligence source renewals will be made on the appropriate form. The applicant in all cases should complete this where the source work requires to continue beyond the previously authorised period (including

previous renewals). The renewal of the authorisation should be signed by the authorising officer.

## 6.7.

Where authorisation ceases to be either necessary or appropriate the Authorising Officer and the applicant will cancel an authorisation using the appropriate form.

## 6.8.

Forms, codes of practice and supplementary material are available on the Council's Intranet.

## 6.9.

Any person giving an authorisation for the use of a Covert Human Intelligence Source must be satisfied that:

- Account has been taken of the likely degree of intrusion into the privacy of persons other than those directly implicated in the operation or investigation ('collateral intrusion'). Measures must be taken, wherever practicable, to avoid unnecessary intrusion into the lives of those affected by collateral intrusion. Particular consideration should be given in cases where religious, medical, journalistic or legally privileged material may be involved, or where the communications of a member of a relevant legislature may be involved.

- The authorisation is necessary (see below).

- The authorised surveillance is proportionate (see below).

- Satisfactory arrangements exist for the management of the source.

- In particular when Environmental Health Investigators deploy DAT noise level monitors to assist in any enforcement action in relation to noisy neighbour complaints. These cases should be reviewed on a case by case basis and if necessary the appropriate authorisation sought.

## 6.10.

Authorisation for use of a Covert Human Intelligence Source can only be granted if sufficient arrangements are in place for handling the Source's case. The arrangements that are considered necessary are that:

### 6.10.1.

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).

**6.10.2.**

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).

**6.10.3.**

There will at all times be 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.

**6.10.4.**

The records relating to the use of that Source are maintained by Orkney Islands Council which will always contain particulars of such matters as may be specified in regulations made by the Scottish Ministers.

**6.10.5.**

The records maintained by Orkney Islands Council that disclose 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. The records kept by Orkney Islands Council should be maintained in such a way as to preserve the confidentiality of the Source and the information provided by that Source. There should, at all times, be a designated person within the authority who will have responsibility for maintaining a record of the use made of the Source.

## 6.11. Necessity

An authorisation for the use of a Covert Human Intelligence Source is necessary on grounds falling within section 7 (3) of RIP(S)A if it is necessary (a) for the purpose of preventing or detecting crime or of preventing disorder; (b) in the interests of public safety; or (c) for the purpose of protecting public health.

## 6.12. Effectiveness

Planned undercover operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

## 6.13. Proportionality

The use of Covert Human Intelligence Sources must be proportionate or in terms of section 7(b) of RIP(S)A that the authorised conduct or use is proportionate to what is sought to be achieved by that conduct or use.

A potential model answer would make clear that the following elements of proportionality had been fully considered:

- Balancing the size and scope of the operation against the gravity and extent of the perceived mischief.

- Explaining how and why the methods to be adopted will cause the least possible intrusion on the target and others.

- Whether there are any implications of the authorised conduct for the privacy of others, and an explanation of why (if relevant) it is nevertheless proportionate to proceed with the operation.

- That the activity is an appropriate use of the legislation and the only reasonable way, having considered all others, of obtaining the necessary result.

- Providing evidence of other methods considered and why they were not implemented.

The degree of intrusiveness of an authorisation of a Covert Human Intelligence Source will vary from case to case, and therefore proportionality must be assessed on an individual basis.

## 6.14. Authorisation

All use and conduct of Covert Human Intelligence Sources shall be authorised in accordance with this procedure.

The Authorising Officer must take into account the following issues when considering an application:

- Who is to be deployed as the source.
- What is being proposed.
- Where and when the proposed deployment will take place.
- Whether it is necessary and proportionate.

**6.14.1.**

However, the tasking of a person should not be used as the sole benchmark in seeking an authorisation. It is the activity of the Covert Human Intelligence Source in exploiting a relationship for a covert purpose which is ultimately authorised by RIP(S)A, whether or not that source is asked to do so by the Council. It is possible therefore that a person will become engaged in the conduct of a Covert Human Intelligence Source without the Council inducing, asking or assisting the person to engage in that conduct. An authorisation should be considered, for example, where the Council is aware that a third party is independently maintaining a relationship (i.e. self-tasking) in order to obtain evidence of criminal activity, and the Council intends to make use of that material for its own investigative purposes.

**6.14.2.**

Underlying all of these considerations is the requirement for the Authorising Officer to be satisfied that the terms of the legislation and relevant guidance are met.

**6.14.3.**

The Authorising Officer should clearly complete the “Authorising Officer’s Statement” on the application form, preferably in their own hand, and articulate in their own words what activity they are authorising.

**The Authorising Officer must state explicitly what is being authorised.**

**6.14.4.**

The Authorising Officer must describe and specify what they are granting. This may or may not be the same as requested by the applicant. For the benefit of those operating under the terms of an authorisation, or any person who may subsequently review or inspect an authorisation, it is essential to produce, with clarity, a description of that which is being authorised (i.e. who, what, where, when and how). The Authorising Officer should as a matter of routine state explicitly and in their 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 should specify the details of how and why they consider the application to be both necessary and proportionate.

**Authorisation different from application.**

**6.14.5.**

If an application fails to include an element in the proposed activity which in the opinion of the Authorising Officer should have been included (for example, the return of something to the place from which it is to be taken for some specified activity), or which is subsequently requested orally by the applicant, it may be included in the authorisation; if so, a note should be added explaining why. Conversely, if an Authorising Officer does not authorise all that was requested, a note should be added explaining why. This requirement applies equally to intrusive surveillance, property interference, directed surveillance and CHIS authorisations.

**6.14.6.**

It is important to note that the reactive nature of the work of a Covert Human Intelligence Source, and the need for them to maintain cover, may make it necessary for the Source to engage in conduct which was not envisaged at the time the authorisation was granted, but which is incidental to that conduct. Such incidental conduct is regarded as properly authorised by virtue of sections 1(6)(a), 5 and 7(5) of RIP(S)A, even though it was not specified in the initial authorisation.

**The Senior Responsible Officer should avoid granting authorisations.**

**6.14.7.**

The role of the Senior Responsible Officer is to oversee the competence of Authorising Officers and the processes in use in their public authority. Whilst legislation does not preclude their use as an Authorising Officer, it is unlikely that they would be regarded as objective if they oversee their own authorisations.

**6.14.8.**

Additionally, the Authorising Officer must assess risks to a Source in carrying out the conduct in the proposed authorisation. The risk assessment must be made by the applicant and presented to the Authorising Officer for consideration. A risk assessment is carried out to determine the risk to the Source of any tasking and the likely consequences should the role of the Source become known. The ongoing

security and welfare of the Source, after the cancellation of the authorisation, will also be considered from the outset.

**Use of a Covert Human Intelligence Source with technical equipment.**

**6.14.9.**

A Covert Human Intelligence Source wearing or carrying a surveillance device and invited into residential premises or a private vehicle does not require special authorisation to record activity taking place inside the premises or vehicle. Authorisation for the use of that Covert Human Intelligence Source may be obtained in the usual way.

**6.14.10.**

Applicants should apply within their own line management structure unless other arrangements have been agreed or it is unreasonable or impractical in the circumstances.

# 7. Security and Welfare

The Council, when deploying a Covert Human Intelligence Source, should take into account the safety and welfare of that Source when carrying out actions in relation to an authorisation or tasking, and the foreseeable consequences to others of that tasking. Before authorising the use or conduct of a Covert Human Intelligence Source, the Authorising Officer should ensure that a risk assessment is carried out to determine the risk to the Source of any tasking and the likely consequences should the role of the Source become known. This should consider the risks relating to the specific tasking and circumstances of each authorisation separately and should be updated to reflect developments during the course of the deployment, as well as after the deployment if contact is maintained.

# 8. Time Periods – Authorisations

## 8.1.

Urgent oral authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after 72 hours, beginning with the time when the authorisation was granted or renewed.

## 8.2.

In terms of the Scottish Government's Code of Practice a written authorisation granted by an Authorising Officer will cease to have effect (unless renewed) at the end of a period of 12 months beginning with the day on which it took effect. Authorisations for the deployment of a juvenile Source are for one month.

# 9. Time Periods – Renewals

## 9.1.

Before an Authorising Officer renews an authorisation, they must be satisfied that a review has been carried out of the use of a Source as outlined in paragraph 10.1 of this Procedure.

## 9.2.

If at any time before an authorisation would cease to have effect, the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, they may renew it in writing for a further period of twelve months. Renewals may also be granted orally in urgent cases and last for a period of 72 hours.

## 9.3.

A renewal takes effect at the time at which, or day on which the authorisation would have ceased to have effect but for the renewal. An application for renewal should not be made until shortly before the authorisation period is drawing to an end. Any person who would be entitled to grant a new authorisation can renew an authorisation. Authorisations may be renewed more than once, in necessary, provided they continue to meet the criteria for authorisation. The renewal should be kept/recorded as part of the authorisation record.

## 9.4.

Authorisations for the deployment of a juvenile Source are renewable for a further period or further periods of one month each.

# 10. Review

## 10.1.

The Authorising Officer shall keep all authorisations under constant review and an authorisation will be cancelled immediately the requirement for surveillance ceases. The Authorising Officer should set review dates and ensure that all reviews are carried out immediately after the Source has been deployed with the review period tailored to meet the particular requirements of the investigation. Details of the review and the decision reached shall be noted on the Review Form.

## 10.2.

Particular attention should be given to the need to review authorisations frequently where they involve a high level of intrusion into private life or significant collateral intrusion, or particularly sensitive information is likely to be obtained. At the point when the Council is considering applying for an authorisation, it must have regard to whether the level of protection to be applied in relation to information obtained under the warrant or authorisation is higher because of the particular sensitivity of that information.

### 10.3.

In each case, unless specified by the Investigatory Powers Commissioner's Office, the frequency of reviews should be determined by the Council. This should be as frequently as is considered necessary and proportionate.

### 10.4.

In the event that there are any significant and substantive changes to the nature of the operation during the currency of the authorisation, the Council should consider whether it is necessary to apply for a new authorisation.

## 11. Cancellation

### 11.1.

The Authorising Officer and the applicant must keep each authorisation under review. The applicant must notify the Authorising Officer if they consider that the authorisation is no longer necessary or proportionate. The Authorising Officer must cancel an authorisation if they are satisfied that the use or conduct of the Source no longer satisfies the criteria for authorisation or that procedures for the management of the Source are no longer in place. Where possible, the Source must be informed that the authorisation has been cancelled.

### 11.2.

Where necessary and practicable, the safety and welfare of the Covert Human Intelligence Source should continue to be taken into account after the authorisation has been cancelled and risk assessments maintained. The Authorising Officer will wish to satisfy themselves that all welfare matters are addressed and should make appropriate comment in their written commentary.

## 12. Record Keeping

### 12.1.

Each Service or discrete location within Services must maintain a record of all applications for authorisation (including refusals), renewals, reviews and cancellations. A centrally retrievable record of all authorisations will be held by the Head of Corporate Governance and be regularly updated whenever an authorisation is granted, renewed or cancelled. An application for authorisation cannot proceed until a unique reference number (URN) has been issued by the Head of Corporate Governance, who must have sight of each and every application. The central register shall be kept up-to-date all times. The record should be made available to the relevant Inspector from the Investigatory Powers Commissioner's Office, upon request. These records should be retained for a period of at least five years. Section 8 of the Council's Policy on Use of Covert Human Intelligence Sources contains further details.

### 12.2.

In addition, consideration should be given to maintaining auditable records for individuals providing intelligence who do not meet the definition of a Covert Human Intelligence Source. This will assist the Council to monitor the status of an individual and identify whether that person should be duly authorised as a Covert Human Intelligence Source. This should be updated regularly to explain why authorisation is not considered necessary.

## 13. Security and Retention of Documents

### 13.1.

Documents created under this Procedure are highly confidential and shall be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of data protection legislation, Chapter 8 of the Scottish Government's Code of Practice on Covert Human Intelligence Sources and the Council's RIPSA Data Safeguards Compliance Process.

### 13.2.

Dissemination or copying of material must be limited to the minimum necessary for authorised purposes. The purposes are authorised if the material:

- Is, or is likely to become, necessary for any of the statutory purposes set out in RIPSA in relation to covert surveillance or property interference;
- Is necessary for facilitating the carrying out of the functions of public authorities under RIPSA;
- Is necessary for facilitating the carrying out of any functions of the Investigatory Powers Commission or the Investigatory Powers Tribunal;
- Is necessary for the purposes of legal proceedings; or
- Is necessary for the performance of the functions of any person by or under any enactment.

### 13.3.

The Head of Corporate Governance will maintain the Central Register of Authorisations. Authorising Officers shall notify the Head of Corporate Governance of the grant, renewal or cancellation of any authorisations and the name of the Applicant Officer within one working day to ensure the accuracy of the Central Register.

### 13.4.

The Authorising Officer shall retain the original Authorisation and Renewal Forms until cancelled. On cancellation, the original Application, Renewal and Cancellation forms shall be forwarded to the Head of Corporate Governance with the Authorising Officer retaining a copy.

### 13.5.

The Authorising Officer shall retain the copy forms for a period of three years after cancellation. The Head of Corporate Governance will retain the original forms for at least five years after cancellation. In both cases these will not be destroyed without the authority of the Authorising Officer if practicable.

### 13.6.

All information recovered through the use of a Source which is relevant to the investigation shall be retained for a period of five years after the cancellation of the authorisation 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 operation is cancelled.

## 14. Particulars to be Contained in Records

The following particulars should be contained in the records:

1. The identity of the Source.

2. The identity, where known, used by the Source.

3. Any relevant investigating authority other than the authority maintaining the records.

4. The means by which the Source is referred to within each relevant investigating authority.

5. Any other significant information connected with the security and welfare of the Source.

6. Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a Source that the information in paragraph 5 has been considered and that any identified risks to the security and welfare of the Source have, where appropriate, been properly explained to and understood by the Source.

7. The date when, and the circumstances in which, the Source was recruited.

8. The identities of the persons who, in relation to the Source, are discharging or have discharged the functions.

9. The periods during which those persons have discharged those responsibilities.

10. The tasks given to the Source and the demands made of them in relation to their activities as a Source.

11. All contacts or communications between the Source and a person acting on behalf of any relevant investigating authority.

12. The information obtained by each relevant investigating authority by the conduct or use of the Source.

13. Any dissemination by that authority of information obtained in that way.

14. In the case of a Source who is not an undercover operative, every payment, benefit or reward and every offer of a payment, benefit or reward that is made or provided by or on behalf of any relevant investigating authority in respect of the Source's activities for the benefit of that or any other relevant investigating authority.

## 15. Oversight

The Investigatory Powers Act 2016 establishes an Investigatory Powers Commissioner's Office to provide comprehensive oversight of the use of the powers to which this Procedure applies. This oversight includes inspection visits by Inspectors appointed by the Investigatory Powers Commissioner.

## 16. Complaints

The Investigatory Powers Tribunal has jurisdiction to investigate and determine complaints against public authority use of investigatory powers. Any complaints in respect of the use by the Council of its powers described in this Procedure should be directed to the Investigatory Powers Tribunal. Full details of how to present a complaint are available on the Tribunal's website – https://investigatorypowerstribunal.org.uk/.

# Document control Sheet

### Review / Approval History

| Date | Name | Position | Version Approved |
|---|---|---|---|
| 1 May 2018 | Gavin Mitchell | Head of Legal Services | V1.2– approved at General Meeting of the Council |
| 1 May 2019 | Gavin Mitchell | Head of Legal Services | V1.3 |
| 11 May 2020 | Gavin Mitchell | Head of Legal Services | V1.4 |
| 5 May 2021 | Gavin Mitchell | Head of Legal Services | V1.4 |
| 9 October 2023 | Gavin Mitchell | Head of Legal and Governance | V1.5 |
| 7 October 2025 | Gavin Mitchell | Head of Corporate Governance | V1.6 |

### Change Record Table

| Date | Author | Version | Status | Reason |
|---|---|---|---|---|
| 1 May 2019 | Gavin Mitchell | 1.3. | Final | Amendment of Paragraph 5.3.1. |
| 11 May 2020 | Gavin Mitchell | 1.4 | Final | Reflect observations contained in IPC Inspection Report |
| 9 October 2023 | Gavin Mitchell | V1.5 | Final | Reflect observations contained in P&R Committee report on 19 September 2023 and subsequently ratified by Full Council on 3 October 2023. |
| 7 October 2025 | Gavin Mitchell | V1.6 | Final | Reflect observations contained in P&R Committee report on 23 September 2025 and subsequently ratified by Full Council on 7 October 2025. |

ORKNEY
ISLANDS COUNCIL

# Surveillance through Social Media Policy

**Contents**



Deleted: 76

Deleted: 87

Deleted: 87

Deleted: 98

# 1. Introduction

## 1.1.

This document sets out Orkney Islands Council's policy regarding internet surveillance using Social Media.

## 1.2.

Reference is made to Orkney Islands Council's policies and procedures in respect of covert surveillance and use of covert human intelligence sources (hereinafter collectively referred to as 'the Council's RIPSA policies and procedures'), to which this policy is subsidiary.

## 1.3.

In some circumstances, it may be necessary for Orkney Islands Council employees, in the course of their duties, to access social media websites either by creating covert identities or through the officer's Service identity.

## 1.4.

Directed online surveillance using an officer's private social media account should not be undertaken in any circumstances given the personal and operational security risks which such use would be liable to present.

## 1.5.

Officers are referred to paragraphs 3.11 to 3.16 of the Scottish Government's Code of Practice on Covert Surveillance and Property Interference (December 2017) and paragraphs 4.7 to 4.14 of the Scottish Government's Code of Practice on Covert Human Intelligence Sources (December 2017) which provide operational examples that would assist staff in recognising situations where RIPSA is potentially engaged in their investigations.

## 1.6.

Whilst much of the work undertaken by social workers is not in pursuance of the prevention or detection of crime, and is not within the purview of RIPSA, research conducted online in the interests of a child may still engage an individual's rights under Article 8 of the European Convention of Human Rights (right to respect for one's private and family life). This should be considered by staff prior to conducting any research online, being aware of their obligations in ensuring such Article 8 rights are not infringed by any online research conducted in child protection cases. Therefore, a protocol containing an auditable process has been developed for circumstances where online research is considered necessary in the interests of child protection. The process is similar to the procedure for seeking a RIPSA authorisation as commended by the Investigatory Powers Tribunal. The Orkney Health and Social Care Partnership shall be responsible for ensuring that this process is observed and responsible for adherence to the Safeguards in relation to retention, review and destruction of material obtained in accordance with the Council's RIPSA Data Safeguards Compliance Process.

## 2. Statement of Intent

The aim of this policy is to provide the framework outlining the Council's process for authorising and managing internet surveillance operations using social media, and to set the parameters for expected good practice.

## 3. Objective

The objective of this policy is to ensure that all surveillance through social media conducted by Orkney Islands Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Council's RIPSA policies and procedures, the relevant legislation, the Scottish Government's Codes of Practice on Covert Surveillance and Property Interference and on Covert Human Intelligence Sources ('the Codes of Practice') and any guidance which the Investigatory Powers Commission may issue from time to time.

## 4. Orkney Islands Council's Social Media Presence

The Council has several social media accounts, covering authority-wide and individual service areas or establishments. There are four authority-wide channels - Facebook, X (formerly Twitter), LinkedIn and Instagram. These channels are managed by the Communications team and provide information about a range of Council activities.

## 5. Types of Investigators' Accounts

There are two different ways in which social media websites may be accessed by Council officers to carry out investigations:

- Through an identity created specifically as the service's representative.
- Through a covert identity using a false name.

## 6. Types of Surveillance

Investigators utilise social media in two different ways:

- By simply visiting / viewing third party accounts or groups.
- By entering into a personal relationship with the third party/group member.

## 7. Privacy Settings of Account under Investigation

### 7.1.

Most social media websites will have a variety of privacy settings that users can apply to protect their accounts from others accessing the information contained therein. Facebook would be the social media website that would be most commonly used by Council Officers to investigate service users or potential service users and it has several different privacy settings. Therefore, Facebook will be used as an example in this policy. Depending on what privacy setting a user chooses, different people can access the account and see all or some of its contents.

**7.1.1. 'Public'**

All Facebook users can see the account and all of its content, including the user's "friends", their timeline and photographs. Non-Facebook users can see photographs and posts published on the account, but not who has 'liked' a post or the marital status or geographic location of the user.

**7.1.2. 'Friends'**

Only those whom the user has accepted as Facebook 'friends' are able to see the entire content of the user's page.

**7.1.3. 'Custom'**

The user can create lists of specific contacts and Facebook users and designate them as the audience for – or block them from view of – any posts.

Of these three options, the relevant options for investigating officers are 'public' and 'friends', as option 3 is a sub-category of 'friends'.

# 8. Utilisation of Social Media

## 8.1. Surveillance using identity as department's representative or departmental account

**'Public' privacy setting**

**8.1.1.**

If an investigating officer views a service user's Facebook profile, with whom they are not 'Friends' via a normal route, and where the content is not protected by any privacy settings, then information on this profile can be treated as being in the public domain. If the viewing/visiting of this profile is not specifically targeted, such viewing/visiting will be overt and no authorisation under RIPSA will be required.

**8.1.2.**

Notwithstanding paragraph 8.1.1 above, directed online surveillance may be invoked even where a service user posts publicly. If the officer frequently or regularly views/visits the same individual's profile this must be considered as targeted, particularly where regular views/visits are likely to result in obtaining private information, irrespective of privacy settings. Whilst, strictly speaking, it may be argued that no authorisation under RIPSA for directed surveillance is required in respect of public posts, as a matter of best practice, an appropriate RIPSA authorisation should be sought in such circumstances.

**8.1.3.**

If an investigating officer enters into a 'conversation' with the service user, and if the officer informs them that they are contacting them in their role as an employee of Orkney Islands Council, then this contact will be overt and no authorisation under RIPSA will be required.

**Deleted:** Any

**Deleted:**

**Deleted:**

**Deleted:** However if the service user posts publicly, they can have no expectation of privacy and will give everybody the right to view their posts at any time and as many times as that person wishes to. Therefore,

**Deleted:** . However,

**'Friends' privacy setting**

**8.1.4.**

To investigate a service user whose Facebook account is protected by privacy settings, the investigating officer will have to send the service user a 'friend request'. As it is obvious from the department name that the person behind it is an Orkney Islands Council employee, then the action could not be classified as covert. No RIPSA authorisation would be needed.

**8.1.5.**

In either of the above privacy settings, although the officer has been given access to the account with the consent of the owner, the officer will still need to consider whether the account may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered, particularly where it is intended to monitor the account going forward.

### 8.2. Surveillance using covert identity

**8.2.1.**

If an investigating officer establishes a relationship with a service user under a covert identity in order to obtain, provide access to, or disclose information, then a Covert Human Intelligence Source (CHIS) authorisation will always need to be in place before that is done.

**8.2.2.**

However if a covert identity is presented but no steps are taken to form a relationship with the subject, a CHIS authorisation may not be required. For example, where a website or social media account requires a minimum level of interaction (such as sending or receiving a friend request before access is permitted) this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as "like" or "follow" in order to react to information posted by others online would not in itself constitute forming a relationship. Nonetheless, it should be borne in mind that entering a website or responding to such gestures may lead to further interaction with that user or other users. A CHIS authorisation should be obtained if it is intended to engage in such interaction to obtain, provide access to, or disclose information.

## 9. Best practice for the use of social media in investigations

As a matter of best practice, whenever a Council officer intends to investigate a particular service user through social media, rather than conducting a general sweep of social media sites, an appropriate RIPSA authorisation should be completed.

## 10. Authorisation for all types of surveillance

Please refer to Orkney Islands Council's Policies and Procedures on Covert Surveillance and Use of Covert Human Intelligence Sources.

## 11. Review of Policy

This policy will be reviewed every year from the date of approval.

## Document control Sheet

**Review / Approval History**

| Date | Name | Position | Version Approved |
|---|---|---|---|
| 1 May 2018 | Gavin Mitchell | Head of Legal Services | V1.2– approved at General Meeting of the Council |
| 11 May 2020 | Gavin Mitchell | Head of Legal Services | V1.3 |
| 5 May 2021 | Gavin Mitchell | Head of Legal Services | V1.3 |
| 9 October 2023 | Gavin Mitchell | Head of Legal and Governance | V1.4 |
| 7 October 2025 | Gavin Mitchell | Head of Corporate Governance | V1.5 |
| 16 June 2026 | Gavin Mitchell | Head of Corporate Governance | V1.6 |

**Change Record Table**

| Date | Author | Version | Status | Reason |
|---|---|---|---|---|
| 11 May 2020 | Gavin Mitchell | V1.3 | Final | Reflect observations contained in IPC Inspection Report |
| 7 October 2025 | Gavin Mitchell | V1.5 | Final | Reflect observations contained in P&R Committee report on 23 September 2025 and subsequently ratified by Full Council on 7 October 2025. |
| 16 June 2026 | Gavin Mitchell | V1.6 | Final | Reflect enhancement suggested by IPCO Inspector and outlined in P&R Committee report on 16 June 2026. |

Appendix 8

# Equality Impact Assessment

The purpose of an Equality Impact Assessment (EqIA) is to improve the work of Orkney Islands Council by making sure it promotes equality and does not discriminate. This assessment records the likely impact of any changes to a proposal or changes by anticipating the consequences and making sure that any negative impacts are eliminated or minimised and positive impacts are maximised.

Should you have any questions or wish for your draft EqIA to be reviewed by our Equality, Diversity and Inclusion Adviser, please contact OD@orkney.gov.uk.

| 1. Identification of the Proposal or Change | |
|---|---|
| Name of proposal or change being assessed. | Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) – Review of Policies and Procedures |
| Responsible Service and Directorate. | Chief Executive's Service |
| Date of assessment. | 16 May 2026 |
| Is the proposal or change existing? (Please indicate if the service is to be deleted, reduced or changed significantly). | Review of existing policies and procedures |

| 2. Primary Information | |
|---|---|
| What are the intended outcomes of the proposal or change? | To ensure policies and procedures comply with legislation, relevant guidance and practice. |
| Is the proposal or change strategically important? | Strategic plans include major investment plans, new strategic frameworks or plans such as annual budgets, locality plans or corporate plans. Where a proposal is identified as strategic, evidence relating to socio-economic impacts and inequalities will be required in the relevant section<br>**No.** |

| | |
|---|---|
| State who is or may be affected by this proposal or change, and how? | Council officers who have statutory powers of surveillance.<br>Members of the public who may be subject to surveillance.<br><br>The policies and procedures regulate how these activities may be carried out and ensure that all relevant legal provisions are complied with. |
| How have stakeholders been involved in the development of this proposal or change? | The policies and procedures reflect advice from the Investigatory Powers Commissioner's Office and best practice as set out in Codes of Practice and guidance published by the Scottish Government, produced following consultation with a range of stakeholders including local authorities. |
| Is there any existing data and / or research relating to equalities issues in this policy area? Please summarise.<br>E.g. consultations, national surveys, performance data, complaints, service user feedback, academic / consultants' reports, benchmarking. | Covert surveillance can only be applied to any person where it is lawful, necessary and proportionate. Equality monitoring has not been undertaken on those previously subject to covert surveillance.<br>Article 8 of the Human Rights Act 1998, the right to respect the private and family life, home and correspondence, is a qualified right and, as such, the right is subject to restrictions which are in accordance with the law, necessary and proportionate to achieving a legitimate aim, including the prevention of disorder and crime. Adhering to the terms of the policies and procedures will help ensure that any interference with Article 8 rights satisfies those criteria. These matters are included in bespoke training sessions provided to relevant officers. |
| Is there any existing evidence relating to socio-economic disadvantage and inequalities of outcome in this policy area? Please summarise.<br>E.g. For people living in poverty or for people of low income. See The Fairer Scotland Duty Guidance for Public Bodies for further information. | This section is required for all proposals relating to strategic decisions.<br><br>Not applicable. |
| Could the proposal or change have a differential impact on any of the following equality areas? | Please provide any evidence – positive impacts / benefits, negative impacts and reasons: |

| | |
|---|---|
| 1. Race: this includes ethnic or national groups, colour and nationality. | None identified. |
| 2. Sex: a man or a woman. | None identified. |
| 3. Sexual Orientation: whether a person's sexual attraction is towards their own sex, the opposite sex or to both sexes. | None identified. |
| 4. Gender Reassignment: the process of transitioning from one gender to another. | None identified. |
| 5. Pregnancy and maternity. | None identified. |
| 6. Age: people of different ages. | None identified. |
| 7. Religion or beliefs or none (atheists). | None identified. |
| 8. Disability: people with disabilities (whether registered or not). | None identified. |
| 9. Marriage and Civil Partnerships. | None identified. |
| 10. Caring responsibilities | None identified. |
| 11. Socio-economic disadvantage. | None identified. |
| 12. Care experienced. | None identified. |

| 3. Impact Assessment | |
|---|---|
| Does the analysis above identify any differential impacts which need to be addressed? | No |

| | |
|---|---|
| Does the analysis above identify any potential negative impacts? | No. If Yes please complete the Equality Impact Assessment Action Plan below |
| Do you have enough information to make a judgement? If no, what information do you require? | Yes |

## 4. Equality Impact Assessment Action Plan

Please complete the following action plan where you have identified any differential impacts or potential negative impacts in Section 3 of the Equality Impact Assessment.

| Impact Identified | Action to be taken | Owner | How will it be monitored | Date Action to be completed |
|---|---|---|---|---|
| | | | | |
| | | | | |

## 5. Sign and Date

| | |
|---|---|
| **Signature:** | [redacted] |
| **Name:** | Gavin Mitchell |
| **Date:** | 16 May 2026 |