POLICY AND AUTHORISATION PROCEDURE ON COVERT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

Version History

Version	Date	Author	Change
1	2020	Miles Watters	
1.1	24 August 2023	Miles Watters	Introduced version history. Updated para 4.4 to removed obsolete references and create new links to COVERT_CODE Confirmed by RIPSA Working Group on 24 August 2023

Document Authors

Miles Watters: Freedom of Information & Data Protection Manager

THE HIGHLAND COUNCIL: POLICY AND AUTHORISATION PROCEDURE ON COVERT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

1.0 INTRODUCTION

1.1. In some circumstances, it may be necessary for 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, or to instruct third parties to do so on the Council's behalf. 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) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) together provide a legal framework both for authorising covert surveillance and covert human intelligence sources ('undercover' officers or informants) by public authorities and for an independent inspection regime to monitor these activities within the United Kingdom.

1.3. Surveillance is covert if, and only if, it is carried out in a manner calculated to ensure that any persons who are subject to the surveillance are unaware that it is or may be taking place. Covert surveillance may be authorised under RIPSA if it is either intrusive or directed.

1.4. Intrusive surveillance is covert surveillance that is carried out in relation to anything taking place on residential premises or in any private vehicle, and that involves the presence of an individual on the premises or in the vehicle or is carried out by a means of a surveillance device**. The Council is not authorised to carry out intrusive surveillance.** Consequently, references in this policy to covert surveillance only apply to directed surveillance.

1.5. The Investigatory Powers Act 2016 regulates investigatory actions in respect of the acquisition of communications data. This is therefore outside the scope of this document.

2.0 OBJECTIVE

2.1. The objective of this policy is to ensure that all Directed Surveillance and Covert Human Intelligence Sources (CHIS) used 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 Codes of Practice on Covert surveillance and property interference [COVERT_CODE] [1] and Covert Human Intelligence Sources [CHIS_CODE] [2] ('the Codes of Practice').

2.2. If the procedures outlined in this policy are not followed, any evidence obtained as a result of the surveillance may be open to challenge. This may result in the Procurator Fiscal deciding not to prosecute the case, or in the case later failing because the evidence is deemed to be inadmissible by the court. The Council may also be vulnerable to legal action by individuals who claim that their right to privacy has been infringed.

[1] https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice (December 2017)

[2] https://www.gov.scot/publications/covert-human-intelligence-sources-code-practice (December 2017)

3.0 COMPLAINTS

3.1. In the event of any member of the public being unhappy or dissatisfied with the conduct of any covert surveillance, in addition to the Council's complaints procedure below, they have the right to complain to the: **Investigatory Powers Tribunal, PO Box 33220, London SW1H 9ZQ**

3.2. Details of the Council's complaints procedure are available at **www.highland.gov.uk/complaints**

4.0 SCOPE OF THE PROCEDURE

4.1. This procedure applies in all cases where directed surveillance or the use of a covert human intelligence source is being planned or carried out.

4.2. Directed surveillance is defined 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' [COVERT_CODE paragraph 2.4].

4.3. The procedure does not apply to observations that are not carried out covertly, or to unplanned observations made as an immediate response to events. As a result, it does not apply to the use of overt CCTV systems unless these systems are used as part of a pre-planned operation or investigation, in which event authorisation may be necessary. Equally, this procedure does not apply to ad-hoc covert observations that do not involve the systematic surveillance of specific person(s). In cases of doubt, the authorisation procedures described below should however be followed.

4.4. Repeated viewing of 'open source' sites may constitute covert surveillance and as such an authorisation may be required. Online covert activity, covert observations and undisclosed engagements on social media must be conducted with full regard to paragraphs 3.11-3.16 of the COVERT_CODE as well as observing the necessity, proportionality, and collateral intrusion principles [COVERT_CODE 4.7-4.14].

4.5. A covert human intelligence source is defined as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that: -

a. covertly uses such a relationship to obtain information or to provide access to any information to another person; or

b. covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship. [CHIS_CODE paragraph 2.1]

5.0 PRINCIPLES OF SURVEILLANCE

5.1. In planning and carrying out directed surveillance or using or conducting a CHIS, Highland Council employees shall comply with the following principles.

5.1.1. Planned directed surveillance/CHIS operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision and authorised under this procedure.

5.1.2. Lawful purposes - directed surveillance or CHIS operations shall only be carried out where this is necessary to achieve one or more of the permitted purposes, i.e. it must be:

i. for the purpose of preventing or detecting crime or the prevention or disorder;

ii. in the interests of public safety; or

iii. for the purpose of protecting public health.

5.1.3. Employees carrying out surveillance shall not cause damage to any property or harass any person. Authorisation of directed surveillance or the use or conduct of a CHIS does not amount to a licence to commit a crime. Any source who acts beyond acceptable limits will not be protected from prosecution by the authorisation.

5.1.4. Necessity - directed surveillance/CHIS operations shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s) in terms of paragraph 5.1.2 above.

5.1.5. Proportionality - the use and extent of directed surveillance/a CHIS shall not be excessive i.e. the methods of surveillance used must not be more intrusive than is warranted by the seriousness of the criminal or undesirable activity under investigation.

5.1.6. 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. The applicant for an authorisation must detail in the application whether it is likely that there will be collateral intrusion and if so, confirm how this will be addressed in some detail. Material which is not necessary or proportionate to the aims for the operation should be discarded or securely retained separately where it may be required for future evidential purposes. The Authorising Officer should ensure appropriate safeguards are in place for the handling, retention or destruction of such material.

5.1.7. Authorisation - all directed surveillance and covert human intelligence sources shall be authorised in accordance with the procedures described below.

6.0 PARTICULAR ISSUES

6.1. Confidential information

6.1.1. RIPSA does not provide any special protection for confidential information. It does however provide for a higher level of authorisation. In operations where confidential information is likely to be involved, authorisation should be sought from the Chief Executive rather than the usual Authorising Officer.

6.1.2. Confidential information includes information subject to legal privilege, confidential personal information and confidential journalistic material. [See CHIS_CODE Chapter 8]. Advice should be sought from the RIPSA Gatekeeper (See paragraph 8.4) if any of these types of confidential information are likely to be involved in an operation.

6.2. Directed surveillance

6.2.1. By definition, directed surveillance intrudes on people's privacy as it will involve obtaining private information about someone.

6.2.2. Private information includes information about a person's private or family life. The concept of private life is broadly interpreted. It includes not only personal information but also information about an individual's relationships with others and can include how they he runs their business and professional affairs. Family life is treated as extending beyond the formal relationship created by marriage. The key issue is likely to be whether there is a reasonable expectation of privacy in the circumstances. If there is, the safest option is to seek authorisation.

6.3. CHIS

6.3.1. A CHIS may include individuals referred to as agents, informants and officers working undercover. The definition of CHIS requires that a relationship is established or maintained. This takes many test purchasing operations outwith this procedure as the carrying out of an everyday transaction does not of itself establish a relationship. If however the intention is for example, for the CHIS to ascertain from the seller details of the supplier of counterfeit goods when the seller took delivery of them etc., that would entail the covert use of a relationship to obtain or provide access to information and would therefore require authorisation.

6.3.2. A number of different terms are used to describe those involved in CHIS operations:

6.3.2.1. Handler – means the person referred to in section 7(6) (a) of RIPSA 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 and
- Monitoring the source's security and welfare

6.3.2.2. Controller – means the person (usually the line manager of the handler) within the local authority referred to in section 7(6)(b) of RIPSA responsible for general oversight of the source. The handler and controller may not be the same person.

6.3.2.3. The conduct of a source means the actions of that source falling within RIPSA or action incidental to it i.e. what the source does.

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

6.3.2.5. Tasking is the assignment given to the source. Either the handler or the controller may task a source. Tasking should be done only after authorisation for the use or conduct of the CHIS has been obtained (usually by way of supplementary Tasking Information Sheets). The only exception to this is where the source will not be establishing or maintaining a relationship for covert purposes, in which case authorisation may not be necessary.

6.3.3. From the above, it may be seen that both the establishment (use) and subsequent utilisation (conduct) of a CHIS require prior authorisation. This is achieved through one application, but care must be taken to ensure that the authorisation satisfies both points [CHIS_CODE paragraphs 2.6 - 2.11].

6.4. Vulnerable individuals or juveniles

6.4.1. Although the safety and welfare of a source must always be taken into account in the risk assessment process, there are special procedures for the use or conduct of vulnerable individuals or juveniles (under 18 years of age) as a source. Reference should be made to the CHIS_CODE in this regard.

7.0 SEEKING AUTHORISATION

7.1. When is authorisation required?

7.1.1. Authorisation is required for directed surveillance (as defined in paragraph 4.2) or the use or conduct of a CHIS (as defined in paragraph 4.5). If in doubt, it is better to obtain an authorisation that proves unnecessary than to jeopardise the admissibility of evidence obtained or risk civil liability on the part of the Council.

7.1.2. Authorisation is required when the activity is carried out by council officers themselves or by third parties carrying out surveillance on behalf of or under the instructions of the Council.

7.1.3. Advice as to whether an authorisation is required may be obtained via the RIPSA Gatekeeper (See paragraph 8.4).

7.2. Who may seek authorisation?

7.2.1. Any officer whose duties involve activity falling within the above descriptions may seek authorisation to do so and must seek authorisation prior to carrying out the surveillance described in paragraph 5.1 above. Before submitting an application for the authorisation or renewal of authorisation for the use or conduct of a CHIS, the officer seeking authorisation must first secure the approval of his or her line manager - as the line manager will be required to act as controller relative to that source.

7.3. When is directed surveillance appropriate?

7.3.1. By its nature, directed surveillance intrudes on people's privacy. It should therefore be regarded as a final option, only to be considered when all other methods have been tried and failed, or when the nature of the suspected activity suggests that there is no other reasonable method which can be used to acquire the information.

7.4. The authorisation process

7.4.1. Applications relative to directed surveillance and the use or conduct of a CHIS shall be authorised by an Authorising Officer listed in Appendix 1 to this policy. Authorising Officers should not be responsible for authorising those operations or investigations in which they may be directly involved

7.4.2. Forms for the application, review, renewal and cancellation of both directed surveillance and the use or conduct of a CHIS are detailed in section 9 below. In urgent cases, an oral application may be approved by the Authorising Officer, although he or she should make a written record of any urgent authorisations granted as soon as practicable thereafter. Urgent authorisations are only valid for a period of 72 hours. If the operation requires to continue beyond the period authorised, in this case 72 hours, a renewal of the application must be authorised before that period has elapsed. Alternatively, the authorisation should be cancelled before the expiry of that period. A case is to be regarded as urgent, so as to permit an authorisation to be given orally, if the time taken to apply in writing would in the judgement of the Authorising Officer be likely to endanger life or to jeopardise the operation for which the authorisation is being given.

7.4.3. There are two situations where only the Chief Executive or (in their absence) their deputy may grant authorisations. The two exceptions are when knowledge of confidential information is likely to be acquired or when a vulnerable individual or a juvenile (under 18 years old) is to be used as a source.

7.4.4. All authorised officers listed in Appendix 1 must be of sufficient seniority as to fall within the scope of the Scottish Government's guidance on authorising grades which is contained in the Regulation of Investigatory Powers (Prescription of Offices etc and Specification of Public Authorities) (Scotland) Order 2010; SSI 2010/350 and any amendments.

8.0 GENERAL DUTIES & SPECIFIC RESPONSIBILITIES OF RIPSA OFFICERS (See Appendix 1)

8.1. Applicants

8.1.1. When completing an application, officers must ensure that the Authorising Officer is provided with all relevant information upon which they should be asked to reach their decision [CHIS_CODE paragraph 5.13].

8.2. Executive Chief Officers (ECOs)

8.2.1. All ECOs are responsible for the dissemination of this policy and ensuring that officers conducting activities covered by RIPSA are aware of the legal implications on the Council of non-compliance.

8.3. Authorising Officer

8.3.1. The Authorising Officer shall be responsible for:

- Deciding whether to authorise directed surveillance (as defined in paragraph 4.2) or the use or conduct of a CHIS (as defined in paragraph 4.5) and ensuring that the authorisation is necessary for the period of the authorisation
- Diarising dates for reviews and renewals and ensuring that these are completed on schedule
- Refusing or cancelling authorisations where appropriate
- Completing the designated forms and conveying relevant documentation to the RIPSA Gatekeeper (See paragraph 8.4) in order to maintain a central RIPSA register.

8.4. Gatekeeper

8.4.1. The Gatekeeper is the Head of Corporate Governance. The Gatekeeper's role is to promote good practice. The Gatekeeper will be available to offer objective judgement and advice to both applicants and Authorising officers on the interpretation of the Act and to ensure quality assurance.

8.4.2. The Gatekeeper is responsible for maintaining a central RIPSA register. The documents in the register shall include:

- A copy of the application and authorisation together with any supporting documentation (including CHIS risk assessments) and notification of the approval given by the Authorising Officer
- A copy of any application for renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested
- A record of the reviews scheduled by the Authorising Officer together with the results of any reviews of the authorisation including any cancellations and the reasons for these
- The reasons for any refusals of authorisation and the reasons, if any, for not renewing an authorisation
- The date and time when any instruction was given by the Authorising Officer to cease using a source and similarly when any instruction stating that directed surveillance should be discontinued

- A Matrix showing abbreviated details of all authorisations including the name, rank/grade of the Authorising Officer, the unique reference number (URN) of the investigation or operation, the title of the investigation or operation

8.4.3. The Gatekeeper shall maintain a RIPSA information page on the Highland Council Intranet incorporating relevant forms and guidance. The Gatekeeper shall also operate a dedicated RIPSA email mailbox.

8.5. Senior Responsible Officer

8.5.1. The codes of practice provide for the role of Senior Responsible Officer (SRO). The duties associated with this role include:

- The integrity of the process in place within the public authority for the management of CHIS and directed surveillance authorisations
- Compliance with RIPSA and the Codes of Practice
- Oversight of the reporting of errors[3] to the Investigatory Powers Commissioner's Office (IPCO) and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors
- Engagement with the IPCO inspectors when they conduct their inspections, where applicable; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by IPCO.
- Report regularly to the Audit and Scrutiny Committee

8.6. RIPSA Working Group

8.6.1. Highland Council's RIPSA Working Group comprises officers from services most involved with RIPSA. The working group will be coordinated by the Gatekeeper and chaired by the Senior Responsible Officer.

8.6.2. The group will meet regularly to perform the following functions:

- To ensure that there is a high standard of training across the Council for relevant officers including cross-service training
- To keep this policy and procedure under review, including advising the SRO of any amendments necessary to the approved forms detailed in section 9
- To be consulted on reports of the IPCO Commissioner, Internal Audit or any other reports concerning RIPSA

[3] https://www.ipco.org.uk/docs/OSC%20PROCEDURES%20AND%20GUIDANCE.pdf#page=23 (Paragraph 79)

8.7. CHIS Handler

8.7.1. The relevant CHIS handler will be responsible for maintaining the details required in terms of The Regulation of Investigatory Powers (Source Records) (Scotland) Regulations 2002; SSI No. 205 and any amendment thereof. Records to be maintained are:

- The identity of the source
- The identity, where known, used by the source
- Any relevant investigating authority other than the authority maintaining the records
- The means by which the source is referred to within each relevant investigating authority
- Any other significant information connected with the security and welfare of the source
- Any confirmation made by a person granting or renewing an authorisation for the conduct or use of a source that the information in the preceding bullet point 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
- The date when and the circumstances in which the source was recruited
- The identities of the persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 7(6) (a) to (c) of RIPSA [i.e. the handler, the controller and the person responsible for maintaining a record of the use made of the source] or in any order made by the Scottish Ministers under section 7(2)(c)
- The periods during which those persons have discharged those responsibilities
- The tasks given to the source and the demands made of him or her in relation to their activities as a source
- All contacts or communications between the source and a person acting on behalf of any relevant investigating authority
- The information obtained by each relevant investigating authority by the conduct or use of the source
- Any dissemination by that authority of information obtained in that way
- Any payment, benefit or reward and every offer of a payment, benefit or reward that is made 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
- Any risk assessment made in relation to the source
- The circumstances in which tasks were given to the source
- The value of the source to the investigating authority

9.0 CONTROLLED DOCUMENTS

9.1.1. This procedure requires the use of specific forms, copies of which are available on the RIPSA pages of the Highland Council's Intranet. No other style of form may be accepted by the Authorising Officer. Forms are approved and agreed by the Senior Responsible Officer in consultation with the RIPSA working group.

10.0 REVIEW, RENEWAL AND CANCELLATION OF AUTHORISATIONS

10.1. Directed Surveillance

10.1.1. A written directed surveillance (DS) authorisation granted by an Authorising Officer will cease to have effect (unless renewed or cancelled) at the end of a period of three months beginning with the day when the authorisation granted has taken effect.

10.1.2. Urgent oral DS authorisations or written DS 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 DS authorisation granted had taken effect.

10.1.3. The Authorising Officer shall review all DS authorisations at intervals of not more than one month, the review period being determined at the point of authorisation or renewal. The purpose of the review is to monitor the effectiveness of the surveillance and its continued necessity and proportionality.

10.1.4. Authorisations for directed surveillance may be renewed where the Authorising Officer considers that the authorisation continues to be necessary and proportionate. Further considerations in relation to renewals are set out in paragraphs 5.14 - 5.18 of the COVERT_CODE.

10.1.5. The Authorising Officer must cancel the authorisation at any time if they consider that the directed surveillance no longer meets the criteria upon which it was authorised. Those acting under an authorisation must notify the Authorising Officer if they consider that the authorisation is no longer necessary or proportionate, and so should therefore be cancelled. [Paragraphs 5.19 -5.21 of the COVERT_CODE].

10.2. CHIS

10.2.1. A written CHIS authorisation will, unless renewed or cancelled, cease to have effect at the end of a period of 12 months beginning with the day on which it took effect, except in the case of juvenile CHIS.

10.2.2. Authorisations for juvenile sources must be authorised by the Chief Executive (see paragraph 7.4.3). The duration of such an authorisation is one month from the time of grant or renewal (instead of 12 months). For these purposes, the age test is applied at the time of the grant or renewal of the authorisation.

10.2.3. Urgent oral CHIS authorisations or CHIS authorisations granted or renewed 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.

10.2.4. Regular reviews of authorisations should be undertaken by the Authorising Officer to assess whether it remains necessary and proportionate to use a CHIS and whether the authorisation remains justified.

10.2.5. Before an Authorising Officer renews an authorisation, they must be satisfied that a review has been carried out of the use of a CHIS and that the results of the review have been considered. Further considerations in relation to renewals are set out in paragraphs 5.18 to 5.20 of the CHIS_CODE.

10.2.6. The Authorising Officer shall cancel any authorisation as soon as he/she is satisfied that it no longer meets the criterion for authorisation. The Authorising Officer will then check

the arrangements in place to terminate the surveillance and the Handler will then advise the source, if any, involved in the operation [Paragraphs 5.29 – 5.30 CHIS_CODE].

11.0 RISK ASSESSMENT

11.1.1. Risk assessment is a requirement in CHIS operations. This assessment should detail any possible risks to staff or other persons involved in or affected by an operation and should be completed on the Highland Council form approved for this purpose.

11.1.2. Before authorising directed surveillance, the Authorising Officer should consider whether the proposed action would place any employee or other person at risk. If so, the Authorising Officer shall have regard to other council procedures already in place and should also consider the risk assessment of the proposed course of action submitted with the application before authorisation is granted. The ongoing security and welfare of any source after cancellation or expiry of the authorisation should also be considered.

12.0 MONITORING AND REVIEW

12.1.1. It shall be the duty of the Gatekeeper to monitor and review the authorisations granted by the Authorising Officer in terms of paragraph 8.2.1 to ensure that time periods have been observed, renewals and cancellations pursued where appropriate and that sufficient details are contained in applications and authorisations.

13.0 SECURITY AND RETENTION OF DOCUMENTS

13.1.1. Documents created under this procedure are highly sensitive and must be treated as such. The Gatekeeper shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 2018 and the Codes of Practice. It should be noted that refusals as well as approved applications must be retained. RIPSA records will be retained for a period of 5 years from the ending of the authorisation. Refusal records will be retained for five years from the date of refusal.

13.1.2. Each appropriate Council Service shall make proper arrangements for the retention, security and destruction of internal RIPSA documentation and any material obtained by surveillance in accordance with the requirements of Data Protection legislation, the Codes of Practice, and the Council's retention policy. Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained in accordance with established disclosure requirements.

13.1.3. Documents will be inspected periodically by the Investigatory Powers Commissioner's Office, which has statutory powers of inspection.

Appendix 1 - RIPSA Officers

Role	Job Title
Senior Responsible Officer	Executive Chief Officer (Performance & Governance)
Gatekeeper	Head of Corporate Governance
Authorising Officer	Corporate Audit Manager
Authorising Officer	Legal Manager – Litigation & Advice
Authorising Officer	Trading Standards Manager
Applications where Confidential information is likely to be obtained	Chief Executive (or their designated Deputy)
Applications where vulnerable individual or juvenile is to be used as a source.	Chief Executive (or their designated Deputy)