POLICY ON COVERT SURVEILLANCE

Introduction

In some circumstances it may be necessary for Comhairle employees, in the course of their duties, to make observations of a person in a covert manner, i.e. without that person's knowledge. By their nature such actions are potentially intrusive (in the ordinary sense of the word) and may give rise to legal challenge as being a 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).

The Regulation of Investigatory Powers Act 2000 and the Regulation of Investigatory Powers (Scotland) Act 2000 ("RIP(S)A") provide a legal framework for covert surveillance by public authorities and an independent inspection regime to monitor these activities. Use of RIP(S)A is regulated by the Investigatory Powers Commissioner's Office ("IPCO").

Objective

The objective of this Policy is to ensure that all covert surveillance by Comhairle employees is carried out effectively while remaining in accordance with the law. It should be read in conjunction with the following documents:

- Covert Surveillance and Property Interference Code of Practice (Scottish Government, 2017)
- Covert Human Intelligence Sources Code of Practice (Scottish Government, 2017)

Scope of the Policy

This Policy applies in all cases where "directed surveillance" is being planned or carried out. Directed surveillance is defined in s1(2) of RIP(S)A as covert surveillance undertaken:

- for the purposes of a specific investigation or operation;
- in such a manner as is likely to result in the obtaining of private information about a person; and
- otherwise than by an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought.

This Policy does not therefore apply to ad-hoc covert observations that do not involve systematic surveillance. Equally, it does not apply to observations that are not carried out covertly, or to unplanned observations made as an immediate response to events.

However, in cases of doubt the authorisation procedure described below should be followed.

Principles of Surveillance

In planning and carrying out covert surveillance, Comhairle employees should comply with the following principles:

Lawful purposes – covert surveillance shall only be carried out where necessary in order to achieve one or more of the permitted purposes set out in s6(3) of RIP(S)A, which are:

- 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 surveillance shall not cause damage to any property or harass any person.

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

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

Proportionality – the use and extent of covert surveillance shall be as defined in section 6(2) of RIP(S)A, i.e. the authorised surveillance is proportionate to what is sought to be achieved by carrying it out. The issue of proportionality must be addressed in applications for authorisation.

Intrusive surveillance – there shall be no surveillance of any person within the definition of "intrusive surveillance" in section 1(3) of RIP(S)A; that is surveillance of anything taking place on residential premises or in a private vehicle which 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 vehicle.

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.

Authorisation – all directed surveillance requires to be authorised in accordance with the procedure described below.

The Authorisation Procedure

Applications for directed surveillance require to be authorised by the Chief Executive, or in his absence by another specified senior officer. The authorising officers are specified in Appendix 1.

The authorising officer must consider the following issues:

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

Underlying all of those considerations is the importance for the authorising officer to be satisfied that the terms of the legislation and relevant guidance are met before authorisation is granted.

In urgent cases, oral applications may be authorised. A case is not normally to be considered urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation in question. An authorisation is not to be considered urgent where the need for authorisation has been neglected or the urgency is of the applicant officer's own making. The applicant officer and authorising officer must complete their records of the oral application and authorisation as soon as practicable.

A written authorisation granted by an authorising officer will, unless renewed, cease to have effect at the end of 3 months beginning with the day on which it took effect. However, the authorised operation is expected to be concluded in as short a time as possible, at which point the authorisation should promptly be cancelled. A review date should be set so that the authorisation can be cancelled when no longer necessary and proportionate.

Urgent oral authorisations will, unless renewed, cease to have effect after 72 hours beginning with the time when the authorisation was granted or last renewed.

Forms

This Policy requires the use of the following forms which are set out in Appendix 2:

<u>1. Application for Written Authorisation</u>
This must be completed by the applicant officer in all cases other than oral authorisations (see 2 below). It is effective from the time that authorisation is given.

<u>2. Record of Oral Authorisation</u>
This should be completed by the applicant officer only in cases where the urgency of the situation makes the submission of a written application impracticable. It must be countersigned by the original authorising officer as soon as possible.

<u>3. Review of Authorisation</u>
A review is an assessment of whether or not an authorisation should be cancelled before its expiry date. It must be completed by the applicant officer at the intervals set out in the original authorisation, and then considered and signed by the authorising officer.

4. Renewal of Authorisation

This must be completed by the applicant officer in all cases where surveillance is sought to be extended beyond the original period of authorisation (including any previous renewals). It is effective from the time that authorisation is given. In every case, the authorising officer must reconsider afresh all of the issues set out below; the authorising officer must also consider in detail the progress of the operation to date.

5. Cancellation

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

Security and Retention of Documents

Documents created under this procedure are highly confidential and should be treated as such. Departments must make proper arrangements for their retention, security and destruction in accordance with the requirements of the Data Protection Act 2018, the Comhairle's Data Protection and Document Retention Policies, and chapter 8 of each of the Codes of Practice.

The Chief Executive is the Comhairle's nominated Senior Responsible Officer and as such has responsibility for:

- the integrity of the authorisation process
- compliance with RIP(S)A and the Codes of Practice
- engagement with IPCO inspectors
- implementation of any post-inspection action

The Monitoring Officer maintains a central register of authorisations. The register contains 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 operation is likely to result in obtaining confidential information as defined in the Codes of Practice
- the date the authorisation was cancelled

The register is updated whenever an authorisation is granted, renewed or cancelled. Applicant officers must send the original of the completed authorisation form to the Monitoring Officer as soon as authorisation is granted. They must also provide subsequent relevant information so as to enable the Monitoring Officer to keep the register up to date.

The register is retained for a period of at least 3 years from the end of the authorisation, and it is made available to IPCO upon request.

Departments should maintain the following documentation, which need not form part of the central register:

- a copy of the application and a copy of the authorisation together with any supplementary documentation and notification of the authorisation 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.

Any concerns or queries about security or retention of documents should be referred to the Monitoring Officer.

Flowchart

A flowchart of the decision-making and recording process is set out at Appendix 3.

Use of the Internet and Social Media

The internet can be a very useful source of information when carrying out investigations. However, staff must be aware that some activities may constitute covert surveillance for which authorisation is required.

Where the process of gathering information entails a general, casual searching of the internet or social media (such as viewing someone's public Facebook page), it is unlikely to be surveillance because it does not involve a systematic monitoring of the person's activity. Therefore, in that situation authorisation would not be required.

However, the use of social media in a systematic way to monitor a person's activities might constitute covert surveillance for which authorisation would be required. Certainly, the setting up of a false or anonymised Facebook account in order to befriend someone and so gain access to further information about that person should never be done without a directed surveillance authorisation. Furthermore, communicating with the site host anonymously so as to obtain further information should not be taken without a CHIS authorisation (see below).

Where the proposed activity falls between those two extremes, staff must be particularly alert to the possibility that it might constitute covert surveillance for which authorisation would be required. Paragraphs 3.11 to 3.16 of the Covert Surveillance and Property Interference Code of Practice, and 4.7 to 4.17 of the Covert Human Intelligence Sources Code of Practice are of assistance on this point. Regardless of the reasons for the activity, it must be demonstrated that it is legitimate and proportionate in order that there is no infringement of Article 8. In the case of any doubt, staff may seek advice from Legal Services or an authorising officer, but it is always safer to seek authorisation than not.

Covert Human Intelligence Sources ("CHIS")

A CHIS is defined in s1(7) of RIP(S)A as a person who establishes or maintains a professional or other relationship with another person for the covert purpose of either:

(i) covertly using the relationship to obtain information or to provide access to any information to another person; or

(ii) covertly disclosing information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A purpose is covert if, and only if, the relationship is conducted in a manner that is calculated to ensure that one of the parties is unaware of the purpose. A relationship is used covertly and information disclosed covertly if, and only if, it is used or disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure.

Therefore, for a person to be a CHIS, they must have established a relationship with another person for a covert purpose.

Use of a CHIS requires to be authorised in a similar way to the use of directed surveillance.

It is not the Comhairle's policy to use CHISs. Members of the public may frequently provide information to the Comhairle about someone whom they believe to be acting illegally or improperly. In most cases, those members of the public will have obtained the relevant information merely by observation; they will not have formed a relationship with the person for the covert purpose of obtaining the information. Therefore, even if they insist on providing the information confidentially or even covertly, it is unlikely that they would be considered a CHIS. However, it is possible that a member of the public has established, or might establish, a relationship with a person for the purpose of obtaining information without that person's knowledge. If that is the case, the member of the public might be a CHIS. Paragraphs 2.18, 2.23 and 2.25 of the Covert Human Intelligence Sources Code of Practice are of assistance on this point.

It is therefore vital that staff are aware of the definition of a CHIS and that, when presented with information from a member of the public, they question how the information was obtained. This is important for two reasons: first, in acting on information from a person who is in reality a CHIS, whether or not authorised as such, the Comhairle owes a duty of care to that person and may put him/her at risk of reprisals; second, the resulting evidence may be ruled inadmissible if the method used to obtain it was not appropriately authorised. Where there is any doubt whether or not someone is a CHIS, staff should seek advice from Legal Services or an authorising officer so that it can be decided if authorisation should be sought.

Appendix 1 – Authorising Officers

1. The Chief Executive in the first instance

2. Where the Chief Executive is absent:

- The Chief Executive's depute
- Any Chief Officer at level CO2 or above

None of the authorising officers are limited to acting only in urgent cases.

Appendix 2 - Forms

- 1. Application for Written Authorisation

Form - application for written authorisation.

- 2. Record of Oral Authorisation

Form - oral authorisation.doc

- 3. Review of Authorisation

Form - review of authorisation.doc

- 4. Renewal of Authorisation

Form - renewal of authorisation.doc

- 5. Cancellation

Form - cancellation of authorisation.doc