Renfrewshire Council

**To: Finance, Resources and Customer Services Policy Board**

**On: 5 June 2019**

**Report by: Director of Finance and Resources**

**Subject: Revised Policy and Guidelines on Surveillance**

## 1. Summary

1.1 The Council's Policy and Guidelines on Surveillance was first approved by the General Management Policy Board on 19th December 2001 and has been subject to review by the General Management and Finance Policy Board on January 2008, January 2011 and August 2014. It was further reviewed by the Finance and Resources Policy Board in May 2016 and is now due its three yearly review, which has been recognised as good practice by the Office of Surveillance Commissioners ("OSC") during Council inspections.

1.2 Only minor amendments are required, predominantly to reflect changes to Council structure. The revised Policy also takes account of the fact that the work previously conducted by the OSC, in relation to overseeing public authority use of covert surveillance, is now carried out by the Investigatory Powers Commissioner's Office ("IPCO").

## 2. Recommendations

It is recommended that the Board:-

2.1 Approve the revised Policy and Guidelines on Surveillance which form the Appendix to this report and continue to authorise the Managing Solicitor (DPO) to update the guidance note appended to the Policy, as required.

2.2 Note the contents of the Report, in particular, paragraph 5, regarding the number of applications for surveillance authorised by the Council in the last three years.

## 3. Background

3.1 The Human Rights Act 1998 obliges all public authorities to act in a manner compatible with the rights contained in the European Convention of Human Rights. The Regulation of Investigatory Powers (Scotland) Act 2000 ("RIPSA") provides a legal framework for covert surveillance by public authorities. If RIPSA is complied with, any interference with the right of privacy contained in the European Convention will be in accordance with law.

## 4. Renfrewshire Council's Policy

4.1 Renfrewshire Council's Policy and Guidelines, first approved in 2001, as amended in 2008, 2011, 2014 and 2016, outlines the procedures which should be followed when the Council is carrying out covert surveillance, making it easier for Council officers to ensure compliance with RIPSA and thus the Human Rights Act. Only minor revisals to the existing Policy have been made. The main changes, highlighted in bold, for ease of reference, relate to updates to the designations of officers who can authorise covert surveillance, further to changes to the Council structure and the role of IPCO. The Policy also takes account of the most recent revisions to the Scottish Ministers' Code of Practice on Covert Surveillance and Property Interference.

## 5. Number of Authorisations

5.1 The Council is committed to compliance with RIPSA and the Human Rights Act 1998. As such, only surveillance which is lawful, necessary and proportionate is ever authorised. Only one authorisation has been granted in the last three year period.

---

**Implications of the Report**

1. **Financial** - None

2. **HR & Organisational Development** – None

3. **Community Planning –** None

4. **Legal** - The Council's revised Policy and Guidelines continue to ensure compliance with the Regulation of Investigatory Powers (Scotland) Act 2000 and the Human Rights Act 1998.

5. **Property/Assets** – None

6. **Information Technology** – None

7. **Equality & Human Rights** -The Recommendations contained within this report have been assessed in relation to their impact on equalities and human rights. The purpose of the report is to ensure compliance with the Human Rights Act 1998. No negative impacts on equality groups or potential for infringement of individuals' human rights have been identified arising from the recommendations contained in the report. If required following implementation, the actual impact of the recommendations and the mitigating actions will be reviewed and monitored, and the results of the assessment will be published on the Council's website.

8. **Health & Safety** – None

9. **Procurement** – None

10. **Risk –** The revised Policy supports the management of risk in relation to avoidance of any human rights breach.

11. **Privacy Impact** – None

12. **COSLA Policy Position –** Not applicable

---

**List of Background Papers**

(a) Background Papers - None

---

**Author**: **Allison Black, Managing Solicitor (DPO) Ext 7175**

Renfrewshire Council

# POLICY AND GUIDELINES

# on

# SURVEILLANCE

## Document Details

| | |
|---|---|
| **Title** | Surveillance Policy and Guidelines |
| **Author** | Allison Black, Managing Solicitor (Information Governance) |
| **Issue Date** | December 2001, most recently updated June 2019 |
| **Subject** | |
| **Description** | |
| **Version** | 6 |
| **Source** | |
| **Updating Frequency** | Three yearly, or earlier if required to reflect legislative change or relevant guidance. |
| **Right** | |
| **Category** | |
| **Identifier** | |

## Document History

| Version | Date | Author | Reason for Issue / Change |
|---|---|---|---|
| 6 | April 2019 | Alison Black | Review |
| 5 | May 2016 | Allison Black | Updated guidance on use of social media and information volunteered |
| 4 | 2014 | Allison Black | OSC recommendations |
| 3 | January 2011 | Allison Black | OSC recommendations |
| 2 | January 2008 | Allison Black | OSC recommendations |

## Related Documents

| Ref | Document Name/ Version | Document Location |
|---|---|---|
| | | |
| | | |
| | | |

## Document Review and Approval

| Name | Action | Date | Communication |
|---|---|---|---|
| Gerard Hannah | | | Email |
| Andrea McMahon, Chief Auditor | | | Email |
| Karen Campbell<br>Chris Dalrymple | | | Email |
| Maxine Hendry,<br>Tom Irvine, | | | Email<br>Email |

**RENFREWSHIRE COUNCIL**

**POLICY AND GUIDELINES ON SURVEILLANCE**

## PART 1 - BACKGROUND

### 1.1 INTRODUCTION

In some circumstances it may be necessary for Council employees, in the course of their duties, to make observations of a 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. Actions of this sort are potentially intrusive. The Human Rights Act 1998 obliges all public authorities to act in a manner compatible with the rights contained in the European Convention of Human Rights ("the Convention"). Article 8 of the Convention affords everyone the right to respect for private and family life including home and correspondence. Surveillance activities by public authorities may therefore result in a legal challenge in terms of Article 8.

Article 8 of the Convention is not however an absolute right. Interference with this right of privacy may be justified if this is:

- in accordance with law;
- necessary to pursue a legitimate aim, for example, the public interest; and
- the interference is proportionate to the legitimate aim, i.e. the interference with the right is not greater than is necessary to achieve the aim.

The Regulation of Investigatory Powers (Scotland) Act 2000 ("RIPSA") provides a legal framework for covert surveillance by public authorities and an independent inspection regime to monitor these activities. If RIPSA is complied with, any interference with the right to privacy will be in accordance with law. As long as the action taken is also necessary and proportionate there will be no breach of Article 8 of the Convention.

### 1.2 OBJECTIVES

The objective of this policy is to ensure that all covert surveillance by Council employees is carried out effectively, legally and proportionately. This policy should be read in conjunction with the Scottish Ministers' revised Code of Practice on Covert Surveillance and Property Interference ("the Code of Practice") and any amendments thereto.

If the procedures outlined in this policy are not followed, any evidence acquired as a result of surveillance activities may be susceptible to a human rights challenge. As a result, it may not be admissible in court, and the Procurator Fiscal is unlikely to take proceedings on the basis of such evidence. The Council may also be exposed to legal action for any breach of human rights.

## 1.3 SCOPE OF THE POLICY

The policy only applies where surveillance is covert i.e. carried out without the knowledge of the subject. It does not apply to observations or surveillance that is not carried out covertly, e.g. use of overt CCTV cameras, or unplanned observations made as an immediate response to events. It should be noted however, that although use of CCTV is generally classed as overt surveillance, due to the presence of signage, alerting the public to the fact that they are being monitored, if CCTV operators decide that targeted surveillance of a specific subject(s) or for a particular investigation becomes necessary, then this could fall within the definition of directed surveillance and an authorisation should be obtained in accordance with this policy. **Similarly, wearing a uniform (for example, a Council warden) does not of itself make surveillance overt if this is specific and targeted.**

### Directed Surveillance

The policy applies in all cases where "directed surveillance" is being planned or carried out. Directed surveillance is covert surveillance undertaken "for the purposes of a specific investigation" and "in such a manner as is likely to result in the obtaining of private information about a person". The policy does not apply to further activities undertaken by the Council as a result of information discovered through the use of surveillance.

### Intrusive Surveillance

RIPSA does not permit the authorisation by council officers of intrusive surveillance. Intrusive surveillance means surveillance in relation to any residential premises (but not common areas such as common stairs and closes) or in any private vehicle.

Some additional points should be made about intrusive surveillance. Surveillance is not intrusive if directed into a home or private vehicle from outside unless the information is consistently of the same quality as a device actually present in the home or vehicle would provide. **Previous** advice from the Office of Surveillance Commissioners (“OSC”), which is currently in use by the Investigatory Powers Commissioner’s Office (“IPCO”), suggests that the sort of surveillance undertaken by the Council is unlikely to reach this level of sophistication. Thus activities such as filming goods being sold from the back of a car, or monitoring the level of noise generated by an anti-social tenant (but not the actual words) are unlikely to be classed as intrusive, and so, these activities can be safely carried out, subject to appropriate authorisation. Furthermore, devices, such as listening and audio visual equipment, carried into a home or a private vehicle by a Covert Human Intelligence Source(“CHIS”) do not constitute intrusive surveillance as long as the CHIS has been invited in. However, the device must not be left behind when the CHIS leaves the premises or vehicle. Services are reminded of the need to have proper authorisation before any use is made of a CHIS.

**Covert Human Intelligence Sources**

A "Covert Human Intelligence Source" or "CHIS" is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of either using the relationship to obtain information or to provide access to any information. The principles outlined in this policy are fully applicable to such undercover operations, which must meet the same tests as directed surveillance and be properly authorised. However, additional rules apply to the use of a CHIS, as outlined at 2.2.2 of this policy and in the question and answer briefing note on use of a CHIS, annexed as Appendix A. For this reason, any Service considering use of a CHIS should first consult Legal and Democratic Services.

Council officers making undisclosed site visits or straightforward test purchases do not count as CHIS (as this does not involve the establishment or maintenance of a relationship) and such activities do not require formal authorisation.

Particular care should be taken when a member of the public is acting as an informant. If information is simply volunteered, no application for CHIS is required, as there is no relationship established or maintained for the purposes of obtaining that information covertly**.** Information is volunteered by members of the public to the Council across a number of its functions and for a variety of reasons, from supplementing complaints, to concerned relatives highlighting potential issues to Children's Services**.** However, if the member of the public is asked to make contact or maintain an existing relationship to obtain information, an authorisation for CHIS will be needed, as he/she is establishing or maintaining a relationship to covertly obtain private information. In such cases, sufficient safeguards, as outlined in 2.2.2, must be in place to protect the source and consideration must be given to the risk of reprisals if the information covertly supplied is used as a basis for further action. Services should consult Legal and Democratic Services before using any information obtained in this way.

## 1.4 PRINCIPLES OF SURVEILLANCE

In planning and carrying out covert surveillance, Council employees must comply with the following principles:

- lawful purposes - covert surveillance shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in RIPSA) i.e., it must be:

  (a) for the purpose of preventing or detecting crime or the prevention of disorder;

  (b) in the interest of public safety; or

  (c) for the purpose of protecting public health.

Employees carrying out surveillance should 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 required objective i.e. one of the above lawful grounds of surveillance

- effectiveness - planned covert surveillance shall be undertaken only by, or under the supervision of, suitably trained or experienced employees.

- proportionality - the use and extent of covert surveillance shall not be excessive i.e. the aim could not have been achieved by less intrusive means. Further information on proportionality is provided at paragraph 2.7

- intrusive surveillance - no surveillance shall be undertaken which comes within the definition of "intrusive surveillance".

- collateral intrusion - reasonable steps shall be taken to minimise the acquisition of information that is not directly necessary for the purposes of an investigation and operation being carried out.

- authorisation - all surveillance must be authorised in accordance with the procedures described below.

## PART 2 - THE AUTHORISATION PROCESS

### 2.1 Who may seek an authorisation?

Any officer whose duties involve directed surveillance or use of a CHIS may seek authorisation to do so and must seek and be granted authorisation prior to carrying out the surveillance. This is most likely to arise in Services responsible for policing, enforcement or security functions.

### 2.2 Who may grant/refuse an authorisation?

#### 2.2.1 Directed Surveillance

Authorisation will be granted/refused by the Chief Executive, the Director of **Environment & Infrastructure**, the Director of Communities, Housing and Planning Services, **the Head of Communities and Public Protection, the Communities and Regulatory Manager, the Head of Corporate Governance**, the Infrastructure, Transportation and Change Manager the Chief Auditor and **the Homeless and Housing Support Services Manager.** Authorisation levels are prescribed by the Regulation of Investigatory Powers (Prescription of Officers, Ranks and Positions) (Scotland) Order 2000. In relation to local authorities, the Regulations refer to Assistant Head of Service and Investigation Manager, titles which are little used within Councils. Where possible, there should be at least two organisational tiers of separation between

the applicant and the authorising officer. Authorising Officers must not authorise investigations or operations in which they are directly involved unless this is unavoidable, for example, when it is necessary to act urgently.

2.2.2 Urgency

Applications should be made in writing using the approved form. In urgent cases, however, oral applications may be approved by the Chief Executive, the **Director of Environment & Infrastructure, the Director of Communities. Housing and Planning Services and the Communities and Regulatory Manager**. In any such cases, a statement that the Authorising Officer has expressly authorised the action and the considerations in doing so should be recorded as soon as is reasonably practicable. Where an urgent application is made this should be renewed or cancelled within 72 hours.

A case is not normally regarded as urgent unless the time that would elapse before the Authorising Officer was available to grant the authorisation would, in the judgment of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation for which the authorisation was being given.

An authorisation is not to be regarded as urgent where the need for an authorisation has been neglected or the urgency is of the Authorising Officer's own making.

2.2.2 **Covert Human Intelligence Sources**

The process for granting authorisations for the use or conduct of CHIS is the same as for directed surveillance. In addition, however, authorisations for use of a CHIS can only be granted if sufficient arrangements have been in place for handling the source's case. The arrangements therefore considered necessary are that:-

(1) there will at all times be an appropriate officer within the Council who will have day to day responsibility for dealing with the source on behalf of the Council and for the source's security and welfare (the handler).

(2) there will at all times be another person who will have general oversight of the use made of that source (the controller).

(3) there will at all times be a person who will have responsibility for maintaining a record of the use made of that source. This should be an authorising officer.

The record relating to the use of that source maintained by the Council will always contain particulars of such matters as may be specified in regulations made by the Scottish Ministers.

The records maintained by the 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.

### 2.2.3 **Juvenile Sources**

There are special safeguards in relation to the use or conduct of juvenile sources i.e. sources under the age of 18 years and some additional rules for under 16s. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him. Officers must ensure that an appropriate adult is present at any meeting with the source if the source is under 16 years old. Authorisations for use of a juvenile source must be granted by the Chief Executive.

When dealing with juvenile sources i.e. under 18s, a full risk assessment considering 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 must be identified and evaluated. The nature and magnitude of any risk of psychological distress to the source must also be identified and evaluated. Any such risks must be justified and properly explained to and understood by the source and the officer granting or renewing the authorisation must know whether the relationship to which the conduct or use would relate is between the source and a relative, guardian or person with responsibility for the source's welfare. If it is, particular consideration must be given to whether the authorisation is justified in light of that fact.

### 2.2.4 **Vulnerable Individuals**

A "vulnerable individual" is a person who is or who may be in need of community care services by reason of mental or other disability, age or illness and who is unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any such individual should only be authorised to act as a source in the most exceptional circumstances. In any such cases, authorisations must be granted by the Chief Executive.

## 2.3 **Granting and recording authorisations and refusals**

The authorising officer's job is to be satisfied that the applicant has correctly identified the lawful purpose for the proposed surveillance, has planned the

operation properly so as to minimise collateral intrusion and the collection of confidential information, is not proposing to stray beyond permissible bounds of directives and has correctly applied the proportionality test. Only if satisfied with these points should the authorisation be granted. Any restrictions imposed on the authorisation should be noted as authorising officer comments.

## 2.4 Receipt and logging of applications

All departments carrying out surveillance activities must forward all relevant documentation to the Head of **Corporate Governance**, who is the Senior Responsible Officer ("SRO") in order that a central register detailing the surveillance activities carried out by the Council can be maintained. This confidential register will be open to inspection by the **Investigatory Powers Commissioner's Office ("IPCO"), who now exercise the oversight previously exercised by the Office of Surveillance Commissioners ("OSC").** This represents evidence of the Council's compliance with the law and the Scottish Ministers' Code of Practice.

## 2.5 Duration, renewal, review and cancellation of authorisations

An authorisation for directed surveillance lasts for three months. The authorising officer should note the time and date of the grant/refusal of the application on the relevant form. However, if the reasons justifying carrying out the surveillance cease to apply, then the authorisation should be cancelled and the cancellation form forwarded to the Head of Legal and Democratic Services for filing on the central register.

If surveillance is to be continued for longer than the original period authorised, it is necessary to have a renewal authorised. The tests applicable to renewals are identical to those for initial applications. A renewal will take effect at the time at which an 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. Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation.

Authorisations for the conduct or use of a CHIS run for twelve months. The ongoing security and welfare of the source, even after cancellation of the surveillance, should be considered before an authorisation is granted, on review and prior to any renewal. Applications for the renewal of the conduct or use of a CHIS should not be granted unless the authorising officer is satisfied that a review has been carried out of the use made of the source during the period since the grant, the task given to the source during that period and the information obtained from the conduct or use of the source and the authorising officer has considered the results of such a review. The authorisation should be cancelled if the person who granted or last renewed an authorisation is satisfied that the authorised conduct is no longer required or no longer satisfies the purpose for which it is granted.

Regular reviews of authorisations should be undertaken to assess the need for the surveillance to continue. The results of a review should be recorded on the central record of authorisations. Authorisations should be reviewed frequently where the surveillance provides access to confidential information or involves collateral intrusion. The Authorising Officer should determine how often a review should take place. This should be as frequently as is considered necessary and practicable

2.6 **When is covert surveillance appropriate?**

Before an application is granted, the authorising officer must be satisfied that the surveillance is necessary, that the action is proportionate with what it seeks to achieve and that the aim could not have been achieved by any other means. There is no "one size fits all" formula for considering whether an authorisation should be granted. Each application for an authorisation must be carefully considered by an Authorising Officer on its own merits and can only be authorised when the particular circumstances justify use of covert surveillance**.**

By its very nature, covert surveillance intrudes on people's privacy and so, the Authorising Officer must be satisfied that there is a necessity to use this. There must be an identifiable offence to prevent or detect before an authorisation can be granted. It should therefore be regarded as a final option, only to be considered when all other methods have either been tried and failed, or where the nature of the activity the surveillance relates to is such that it can be reasonably concluded other action will be able to acquire the information being sought. Thus, for example, if a vending machine is regularly being broken into, consideration should be given to installing overt CCTV cameras with appropriate signage before installing hidden cameras.

Any use of covert surveillance must be proportionate to the objective being pursued.

**2.7 Is use of social media and internet by Council officers covert surveillance?**

2.7.1 Officers must not assume that because monitoring and research of activities via the internet and social networking sites e.g. purchase of illicit goods by Trading Standards officers or monitoring by fraud investigators, is routine or easy to conduct, that no authorisation is needed for this.

2.7.2 Social networking sites are designed to enable users to create profiles and form relationships with other users within that site. Profiles will have varying levels of access and disclosure which are controlled by the user and website administrator e.g. all content may be publicly available or some may be restricted to 'friends'. Not all social networking sites work in the same way and so, care must be taken by officers to understand how the sites being used operate. Where privacy settings/access controls are applied to social media

sites, the author has a legitimate expectation of privacy. If there is any covert use made of internet or social networking sites (i.e. the other party does not know that the enquirer is a Council employee) to support a particular investigation or operation, particularly where any privacy settings are passed, then an authorisation should be considered.

If there is any covert use made of internet or social networking sites (i.e. the other party does not know that the enquirer is a Council employee) to support a particular investigation or operation, particularly where any privacy settings are passed, then an authorisation for directed surveillance should be considered. Where a relationship is established or maintained for the covert purpose of obtaining private information, an authorisation for a CHIS should be considered.

2.7.3 However, officers should not assume that viewing "open source" materials, where there are no such controls in place, for the purposes of an investigation will never require an authorisation because this is publicly available. Repeat viewing of this information may require an authorisation, depending on the circumstances, as this becomes targeted and focused and provide a pattern of lifestyle. Although officers may make overt use of publicly available information, advice should be obtained from the Managing Solicitor (DPO) before repeated viewing of social media sites for investigatory purposes, as targeting users can render overt use covert.

2.7.4 Officers should not set up a false identity for a covert purpose without first obtaining an authorisation. Photographs of other people should never be used without their permission.

2.7.5 Officers must never adopt the identity of a person known to users of the site without explicit permission and without considering the protection of that person.

**2.7.6 Internet searches carried out on the Council's behalf by a third party may still require an authorisation.**

**Proportionality**

Proportionality is a concept of human rights fully designed to ensure that measures taken by the state (and its public authorities, such as the Council) which impact on the rights of citizens are kept within proper bounds.

It means that if the same legitimate end can be reached by means of less intrusion on people's rights, or none at all, then the less intrusive option should be taken. There should also be a reasonable relationship between the seriousness of the issue being addressed and the degree of intrusion into people's rights, although it is insufficient to simply assert that the 'seriousness' of the crime justifies any or every method available.

Covert surveillance involves a potentially serious breach of an individual's right to privacy. Compelling reasons are therefore required to justify this, particularly if the surveillance is to continue for an extended period. Thus surveillance of a staff member on sick leave is likely to be disproportionate if all that is being assessed is a possibly fraudulent claim for a very small amount of statutory sick pay, but it may be proportionate when detecting a fraudulent legal claim against the Council for thousands of pounds.

It is useful to consider how serious the breach sought to be rectified is. For criminal offences the potential sentence may be a useful guide. However, many regulatory offences, while attracting only very small fines, are designed to prevent potentially life threatening occurrences (such as sale of dangerous goods or contaminated food, or the overcrowding of licensed premises). Such factors weigh in favour of surveillance being proportionate.

Guidance from the OSC indicates that four elements of proportionality should be considered:-

- Balancing the size and scope of the operation against the gravity and extent of 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 and
- Evidencing what other methods had been considered and why they were not implemented.

## 2.8 Confidential material and collateral intrusion

Confidential material covers a number of areas: professional legal advice, health information, spiritual counselling, journalistic material and material held under an obligation of confidentiality. So far as possible, surveillance operations should be designed so as to minimise or eliminate the possibility of confidential information being acquired. If confidential information is in fact acquired, special care should be taken to avoid unnecessary disclosure of it. If there is any likelihood that confidential information will be acquired, the authorisation should be granted by the Chief Executive.

Collateral intrusion refers to the fact that very often surveillance operations will inadvertently intrude on the privacy of persons other than those at whom the operation is directed. Operations should be planned so as to minimise or eliminate so far as possible the risk of collateral intrusion, and the extent to which it remains is a factor to consider when determining the proportionality of the operation.

## 2.9 Surveillance by other public authorities and external partners

Council officers are occasionally asked to assist in surveillance operations being conducted by other public authorities such as the police, the Benefits Agency, Customs and Excise etc. In such cases it is for the organisation seeking assistance from the Council to ensure that it has appropriate authorisations in place. These authorisations should be shown to Council staff involved or written confirmation should be given that the authorisations have been duly granted. If the Council is carrying out its own surveillance as part of a joint operation, however, Council officers should arrange for its own authorisations to be put in place too. The OSC have, in the past, indicated that they would prefer one public authority to take the lead in joint operations and for authorisations to be made all inclusive, where possible. There may be occasions when the Council wishes to engage a third party in to conduct covert surveillance on its behalf. When a person who is not an employee of the Council is authorised to conduct covert surveillance on behalf of the Council, he is an agent of the Council. In any such case, the Authorising Officer should obtain written acknowledgement of this agency arrangement and confirmation that the agent will comply with the authorisation.

## 2.10 Security and retention of documents

Documents created under this procedure are highly confidential and shall be treated as such. The Head of Corporate Governance**,** as SRO, shall ensure that the central register is kept secure and shall make proper arrangements for the retention and destruction of documentation in accordance with the requirements of the Data Protection Act law and the Code of Practice. It should be noted that refusals, as well as approved applications, must be retained. The Code of Practice states that although retention of authorisations is required for at least three years from the ending of the authorisation, or longer, if required for ongoing proceedings, retention for five years is recommended to ensure that no records are destroyed until a Surveillance Commissioner has had an opportunity to see them. **The Council adheres to this five year retention period**.

In accordance with guidance issued by the OSC, documents will be inspected periodically by the Head of Corporate Governance, to ensure that consistent approach is being adopted by different Council Services. As **IPCO** now has oversight of RIPSA compliance, they have statutory powers of inspection and all records in the Council's central register (applications, authorisations, cancellations and refusals) must be available for inspection.

## 2.11 Training

Each Service is responsible for ensuring that their staff receive adequate training to deal with the authorisation process and any enquiries. Training,

advice and guidance is available, as required, from Legal and Democratic Services.

## 2.12 Public Access

Copies of the Policy and Codes of Practice will be made available to the public on request.

## 2.13 Complaints

In the event of any member of the public being unhappy or dissatisfied with the conduct of any covert surveillance, in addition to the Council's complaints procedure, they have the right to complain to the Investigatory Powers Tribunal. Copies of the Complaints Procedure will be made available to the public by post or e-mail, on request.

# USE OF A COVERT HUMAN INTELLIGENCE SOURCE (CHIS)
# Questions and Answers

1. **Q: What is a CHIS?**

   A: A CHIS is a person who establishes a relationship with another person for the covert purpose of obtaining information e.g. when acting undercover or when dealing with informants.

2. **Q: Why is it important to have a proper authorisation in place for use of a CHIS?**

   A: Admissibility of evidence depends on whether evidence is fairly and lawfully obtained. An authorisation will provide lawful authority for use of a source.

3. **Q: When is it necessary to obtain an authorisation for use or conduct of a CHIS?**

   A: Officers should obtain an authorisation where the use or conduct of a source is likely to interfere with a person's right to privacy, whether or not that person is the actual subject of the investigation or operation.

4. **Q: Is an authorisation for a CHIS needed in relation to test purchases?**

   A: If a Council officer, or someone acting on his behalf, makes a straightforward test purchase no authorisation is required e.g. If an officer or a juvenile purchases cigarettes from a retailer. This is due to the fact that there is unlikely to be a breach of privacy as the officer or juvenile is simply entering the shop in the same way as any other customer. If, however, the officer or the juvenile develops a relationship with the person from whom he is purchasing to elicit further information, it is likely that an authorisation for a CHIS will be necessary. Alternatively, if the shopkeeper is placed under covert surveillance by the use of a device an authorisation for directed surveillance will be more appropriate.

**5. Q: Is a member of the public who volunteers information a CHIS?**

**A:** There is no 'one size' fits all when deciding whether an authorisation for a CHIS is needed. This will depend on the specific circumstances of any given case. However, officers must know when to seek advice on this**.** Particular care should be taken when a member of the public is acting as an informant. If information is simply volunteered, no

application for CHIS is required, as there is no relationship established or maintained for the purposes of obtaining that information covertly. However, if the member of the public is asked to make contact or maintain an existing relationship to obtain information, an authorisation for CHIS will be needed, as he/she is establishing or maintaining a relationship to covertly obtain private information. In such cases, sufficient safeguards, as outlined in 2.2.2 of the Surveillance Policy, must be in place to protect the source and consideration must be given to the risk of reprisals if the information covertly supplied is used as a basis for further action. Services should consult Legal and Democratic Services before using any information obtained in this way.

6. **Q: What about concerned relatives who report issues to Children's Services?**

Once again, this will depend on the circumstances of the case. Social workers, for example, frequently act on information supplied, often in confidence by relatives of a child. No authorisation is need for this. However, should contact become repeated and regular, this should be kept under review and advice sought, as necessary. Whilst Children's Services exercise their statutory powers and duties overtly, staff should be aware of the difference between overt and covert surveillance.

**7 Is an authorisation for a CHIS needed if internet or social networking sites are used by officers for research or investigation?**

**A:** Do not assume that because monitoring and research of activities via the internet and social networking sites e.g. purchase of illicit goods by Trading Standards officers or monitoring by fraud investigators, is routine or easy to conduct, that no authorisation is needed for this.

Social networking sites are designed to enable users to create profiles and form relationships with other users within that site. Profiles will have varying levels of access and disclosure which are controlled by the user and website administrator e.g. all content may be publicly available or some may be restricted to 'friends'. Not all social networking sites work in the same way and so, care must be taken by officers to understand how the sites being used operate. Where privacy settings/access controls are applied to social media sites, the author has a legitimate expectation of privacy. If there is any covert use made of internet or social networking sites (i.e. the other party does not know that the enquirer is a Council employee) to support a particular investigation or operation, particularly where any privacy settings are passed, then an authorisation for directed surveillance should be considered. Where a relationship is established or maintained for the covert purpose of obtaining private information, an authorisation for a CHIS should be considered.

Officers should not assume that viewing "open source" materials, where there are no such controls in place, for the purposes of an investigation will never require an authorisation because this is publicly available. Whilst an authorisation may not be required for single viewing of publicly available information, repeat viewing of this information may require an authorisation, depending on the circumstances, as this becomes targeted and focused. Although officers may make overt use of publicly available information, advice should be obtained from the Managing Solicitor (Information Governance) before repeated viewing of social media sites for investigatory purposes, as targeting users can render overt use covert.

8. **Will obtaining an authorisation mean that there is no breach of human rights?**

A: Interference with the Article 8 ECHR right to privacy can only be justified if it is lawful, necessary and proportionate. It is therefore essential that the authorisation is necessary for one or more of the lawful grounds for surveillance listed at Answer 9. Proportionality involves balancing the right of the person or persons whose privacy is being infringed with the greater good. The use of a CHIS will not be proportionate if the information which is sought could reasonably be obtained by other, less intrusive, means.

9. **Q: What are the lawful grounds for use of a CHIS?**

A: The lawful grounds are:-

- Prevention and detection of crime or disorder;
- Public safety;
- Protection of public health;
- Any other purpose prescribed in an order made by the Scottish Ministers

10. **Q: What about other people i.e. people who are not the subject of the surveillance?**

A: Authorising officers must take into account the risk of intrusion into the privacy of people who are not the subject of the investigation i.e. collateral intrusion. Measures should be taken, where practicable, to avoid unnecessary intrusion into the lives of those not directly connected with the operation or investigation. The application for use or conduct of a CHIS should include an assessment of the risk of any collateral intrusion and the authorising officer should take this into

account when considering the proportionality of the use and conduct of a source.

11. **Q: What if there is unexpected collateral intrusion?**

A: If the investigation or operation unexpectedly interferes with the privacy of individuals who are not covered by the authorisation, the authorising officer should be informed. If there is a possibility that the original authorisation may be insufficient, consideration should be given to whether a new authorisation is required.

12 **Q: What about the wider community?**

A: Authorising officers and officers applying for authorisations will also need to be aware of any particular sensitivities in the local community where the source is being used and of similar activities being undertaken by other public authorities which could impact on the deployment of the source e.g. police. Consideration should be given to any adverse impact on community confidence or safety that may result from the use or conduct of a source or of information obtained from that source. If an authorising officer considers that conflicts may arise, they should consult a senior officer within the police force area in which the source is deployed. In addition, the authorising officer should make an assessment of any risk to a source in carrying out the conduct in the proposed authorisation.

13. **Q: What if there is a need to carry out surveillance on a potential source?**

A: It may be necessary to deploy directed surveillance against a potential source in order to assess their suitability for recruitment. In such cases, an authorisation for a CHIS 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 the potential source could be followed.

14. **Q: What about "confidential information"?**

A: Confidential information includes matters subject to legal privilege, confidential personal information and confidential journalistic material. RIPSA does not provide any special protection for such information. However, particular care should be taken in cases where the subject of the investigation or operation might reasonably expect a high degree of privacy, or where confidential information is involved.

In cases where the use or conduct of a CHIS is likely to result in confidential information being acquired, authorisations must be granted by the Chief Executive.

Where there is any doubt as to the handling and dissemination of confidential information, advice should be sought from Legal Services.

15. **Q: Can a vulnerable individual be authorised as a CHIS?**

A: A "vulnerable individual" is a person who is or who may be in need of community care services by reason of mental or other disability, age or illness and who is unable to take care of himself, or unable to protect himself against significant harm or exploitation. Any such individual should only be authorised to act as a source in the most exceptional circumstances. **In any such cases, authorisations must be granted by the Chief Executive**.

16. **Q: What about juvenile sources?**

A: There are special safeguards in relation to the use or conduct of juvenile sources i.e. sources under the age of 18 years and some additional rules for under 16s. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility for him. Officers must ensure that an appropriate adult is present at any meeting with the source if the source is under 16 years old.

When dealing with juvenile sources i.e. under 18s, a full risk assessment considering 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 must be identified and evaluated. The nature and magnitude of any risk of psychological distress to the source must also be identified and evaluated. Any such risks must be justified and properly explained to and understood by the source and the officer granting or renewing the authorisation must know whether the relationship to which the conduct or use would relate is between the source and a relative, guardian or person with responsibility for the source's welfare. If it is, particular consideration must be given to whether the authorisation is justified in light of that fact.

17. **Q: How long will an authorisation for a CHIS last?**

A: An authorisation for a CHIS relating to juveniles will only last for one month.

In urgent cases an authorisation is valid for 72 hours. Authorisations may be granted orally for urgent cases, but officers should only authorise on this basis in exceptional circumstances.

In all other cases, an authorisation is valid for 12 months.

18. **Q: What about renewals?**

A: Before an authorising officer renews an authorisation, he must be satisfied that a review has been carried out of the use of a CHIS. This review should include the use made of the source during the period of authorisation, the task given to the source and the information obtained from the source. The results of a review should be recorded on the relevant review form. Authorisations should be reviewed frequently where the use of a source provides access to confidential information or involves collateral intrusion. It is for the authorising officer to determine how often a review should take place. However, this should be as frequently as is considered necessary and practicable.

If at any time before an authorisation would cease to have effect, the authorising officer considers it necessary for the authorisation to continue, he may renew it in writing for a further period of 12 months. Renewals may also be granted orally in urgent cases and last for a period of 72 hours.

The renewal will take effect at the time at 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. Authorisations may be renewed more than once, if necessary, provided they continue to meet the criteria for authorisation.

19. **Q: Why are cancellations important?**

A: The authorising officer who granted or renewed the authorisation must cancel it if he is satisfied that the use or conduct of the CHIS no longer satisfies the criteria for authorisation or that satisfactory arrangements for the source's case no longer exist. Where the authorising officer is no longer available, this duty will fall on the person who has taken over the role of the authorising officer or who is acting as authorising officer. Where necessary the safety and welfare of the source should continue to be taken into account after the authorisation has been cancelled.

20. **Q: How do I manage a source?**

A: Tasking - tasking is the assignment given to the source asking him to obtain information, to provide access to information or to otherwise act for benefit of the Council. Authorisation is required prior to any tasking where this requires the source to establish or maintain a personal or other relationship for a covert purpose.

The officer obtaining the authorisation will have day to day responsibility for:-

- dealing with the source on behalf of the Council;
- directing the day to day activities of the source;
- recording the information supplied by the source; and
- monitoring the source's security and welfare

In some cases, the tasking given to a person will not require the source to establish a personal or other relationship for a covert purpose, e.g. a Trading Standards Officer may be involved in the test purchase of items which have been labelled misleadingly or are unfit for consumption. In such cases, it is for the officers involved to determine where, and in what circumstances, such activity may require authorisation (see also Question 4). If in doubt, advice should be obtained from Legal and Democratic Services.

It is not the intention authorisations are so narrow that a separate authorisation is required each time that a source is tasked. An authorisation may cover, in broad terms, the nature of the source's task. If this changes, then a new authorisation may be needed.

It is difficult to predict exactly what might happen each time a meeting with a source takes place, or the source meets the subject of an investigation. There may be occasions when unforeseen action or undertakings occur. When this happens, this must be recorded as soon as practicable after the event and, if the existing authorisation is insufficient, it should be cancelled and a new authorisation should be obtained before any further action is carried out.

Similarly, where it is intended to task a source in a new way or a significantly greater way than previously identified this must be referred to the authorising officer, who should consider whether a separate authorisation is needed. This should be done before any tasking and the details of such referrals must be recorded.

21. **Q: What about the security and welfare of a source?**

A: When deploying a source, the Council should take into account the safety and welfare of that person, when carrying out actions in relation to the authorisation or tasking and to foreseeable consequences to others of that tasking. Before authorising the use or conduct of a source, the authorising officer should ensure that a risk assessment is carried out to determine the risk to the source and likely consequences should the role of the source become known. The ongoing security and welfare of the source, after cancellation of the authorisation, should also be considered at the outset.

Any concerns about personal circumstances of the source should be brought to the attention of the authorising officer if they might affect:-

- the validity of the risk assessment;
- the conduct of the source; and
- the safety and welfare of the source

The authorising officer should make a decision on whether or not to allow the authorisation to continue further to consideration of such matters.

22. **Q: What is the link between intrusive surveillance and a source wearing or carrying a surveillance device invited into a house?**

A: The Council cannot authorise intrusive surveillance. Placing a surveillance device into residential premises of private vehicles is usually classed as intrusive.

However, a CHIS wearing or carrying a surveillance device who is invited into residential premises or a private vehicle, does not require an additional authorisation to record any activity taking place inside those premises or vehicles which take place in his presence. Authorisation for the CHIS may be obtained in the usual way.