Agenda Item 5

RIPSA

Agenda Item 5

Falkirk Council

Title: **RIPSA**
Meeting: **Executive**
Date: **14 May 2019**
Submitted By: **Director of Corporate and Housing Services**

1. Purpose of Report

1.1. This report updates Executive on the outcome of a recent inspection of the Council's use of RIPSA by a representative of the Investigatory Powers Commissioner's Office, and the actions required following on from that, including approval of an updated RIPSA Policy.

2. Recommendations

2.1. **Executive is asked to:-**

(1) note the outcome of the inspection report;

(2) approve the amended RIPSA Policy; and

(3) note the single authorisation granted under RIPSA in 2018.

3. Background

3.1. In limited circumstances, it may be necessary for Falkirk Council employees, in the course of their duties, to make observations of a person in a covert manner (ie 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 and may give rise to legal challenge. The Regulation of Investigatory Powers (Scotland) Act 2000 (known as **RIPSA**) was introduced to make sure that such surveillance was properly regulated, to ensure compliance with Human Rights legislation. There are statutory codes of practice which sit alongside the Act.

3.2. The Council has a detailed RIPSA Policy in place, along with standard forms which require completion and authorisation by relevant officers within the Council.

3.3. Every 3 years, the Council is subject to an inspection on its use of RIPSA powers by an inspector from the Investigatory Powers Commissioner's Office (**IPCO**), which replaced the Office of the Surveillance Commissioner last year. The Council was subject to an inspection visit on 28th November

2018 and received a report on that from IPCO dated 31st January 2019 (**IPCO Report**).

4. Outcome of Inspection

4.1. The IPCO Report concluded that it had been a "good" inspection that demonstrated that the Council had attained a good standard as regards the legislation and relevant Codes of Practice. The inspector was pleased that the policy had been reviewed and kept up-to-date despite the very infrequent use of the powers by the Council over the last 3 years and also that the recommended forms were in use. Three areas were identified for improvement as set out in the table below, along with our response to IPCO:

Recommendation	Response/progress
Amend policy to clarify which roles are permitted to act as Authorising Officers (AO) and the requirement for prior AO training	Recommendation accepted. Policy amended.
Ensure that there is an annual report to elected representatives on the use of RIPSA and for the representatives to set/endorse Council RIPSA policy	Recommendation accepted in part, as it is not our usual practice to set/endorse policies annually. An Information Bulletin report will be submitted to Council each year on the use of RIPSA, with any policy changes being subject to approval by Executive.
All AOs to make authorisations in line with the requirements of the Code of Practice, ensuring review periods are set, cancellations made and that authorisations sufficiently detail why it is necessary, proportionate and what activity or conduct they are specifically authorising	Recommendation accepted, along with observations on training. We will liaise with neighbouring Councils on training plans/content.

5. Amendment of RIPSA Policy

5.1. Amendments to the policy have been made in light of recommendations and observations in the IPCO Report. In particular, the Policy has been amended as follows:

Para	Amendment
3.8 3.9	Examples added to show how use of the internet in the workplace could potentially result in the need for a RIPSA authorisation.
6.7	Clarification that only Designated Authorising Officers can grant authorisations.

6.13	New paragraph to make clear that applicants for authorisations and operational staff must see a copy of the authorisation once granted so they are in no doubt as to what the authorisation permits (and make a record or note they have done so).
Appendix	Reduction in number of Designated Authorising Officers (plus addition of Chief Executive, as permitted under RIPSA).

5.2. The amended policy was reviewed by the Information Management Working Group on 14 March 2019.

6. Authorisations in 2018

6.1. There was one authorisation granted in 2018. By way of comparison, no authorisations were granted in 2017.

7. Consultation

7.1. The Information Management Working Group has been advised of the outcome of the inspection and has reviewed the amended policy.

8. Implications

Financial

8.1 A more intensive RIPSA training programme may come at a cost but we anticipate being able to share these with neighbouring Councils.

Resources

8.2 The resource implications arising out of the recommendations are restricted to the additional training requirements.

Legal

8.3 Failure to comply with the requirements of RIPSA leaves the Council open to challenge for breach of human rights.

Risk

8.4 Failure to have an appropriate policy and training in place places the Council at risk, although, as noted, the Council makes limited use of RIPSA powers,

Equalities

8.5 No equality and poverty impact assessment is required.

Sustainability/Environmental Impact

8.6 No sustainability assessment is required.

9. Conclusions

9.1 Although the Council makes little use of RIPSA powers, it is important that we keep the RIPSA policy and associated documentation under review and ensure adequate training is in place.

____

Director of Corporate and Housing Services

Author – Wendy Barber, Information Governance Manager, 01324 506124, wendy.barber@falkirk.gov.uk
Date: 2nd April 2019

Appendices

RIPSA Policy

List of Background Papers:

The following papers were relied on in the preparation of this report in terms of the Local Government (Scotland) Act 1973:

- None

FALKIRK COUNCIL

REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000

POLICY AND PROCEDURE ON DIRECTED SURVEILLANCE AND THE USE OF COVERT HUMAN INTELLIGENCE SOURCES

Falkirk Council

Index

1 Introduction

1.1 In some circumstances, it may be necessary for Council employees, in the course of their duties, to monitor 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.

1.2 By their nature, actions of this sort can be intrusive and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights (**ECHR**), which protects people's right to respect for their private and family life, home and correspondence. Article 8 can also cover business and professional records, where those disclose information about the private lives of individuals. The Human Rights Act 1998 requires the Council to act compatibly with the ECHR. Section 6 makes it unlawful for a public authority to act in a manner which is in breach of the ECHR.

1.3 The Regulation of Investigatory Powers Act 2000 (**RIPA**), the Investigatory Powers Act 2016 (**IPA**) and the Regulation of Investigatory Powers (Scotland) Act 2000 (**RIPSA**) together provide the legal framework for authorising both covert surveillance and the use of covert human intelligence sources by public authorities. They also establish an independent inspection regime to monitor the practice of these activities by public authorities in the United Kingdom. The Investigatory Powers Commissioner and his office (IPCO) has responsibility for ensuring public authorities act in compliance with legislation. IPCO has replaced the Office of Surveillance Commissioners.

1.4 This policy relates to the Council's powers and duties under RIPSA, which deals with the regulation of surveillance and the use of covert human intelligence sources (**CHIS**). It does not offer any guidance on the application of IPA or RIPA to Scottish local authorities. Council officers must obtain legal advice before exercising any powers under IPA or RIPA.

1.5 Compliance with this policy will help ensure that the Council meets its obligations under RIPSA and that the rights of third parties are protected. It will also help minimise any reputational risk to the Council and help ensure that information obtained through surveillance operations may legitimately be used for its intended purpose. The Chief Governance Officer is the Senior Responsible Officer for ensuring compliance with this policy and the relevant legislation.

2 Objective

2.1 The objective of this policy and procedure is to ensure that all covert surveillance and uses of CHIS by Council employees is carried out lawfully and effectively. It should be read in conjunction with the Scottish Government's **Codes of Practice** on 'Covert Surveillance and Property Interference' and 'Covert Human Intelligence Sources' (current versions in force from December 2017).

2.2 The carrying out of surveillance operations which interferes with a person's right to respect for private life will breach Article 8 of the ECHR unless it is properly authorised by law. RIPSA provides that the conduct to which it applies will be lawful for all purposes if an authorisation under

RIPSA confers an entitlement to carry out the activity, and the activity is carried out in accordance with the authorisation.

2.3 Activities of the type covered by RIPSA which are not authorised are not lawful. If the procedures outlined below are not followed by Council employees, any evidence obtained as a result of the surveillance or CHIS may be open to challenge in legal proceedings and the Council could be prevented from relying on it. This may result in the Council not being able to take legal action (such as eviction proceedings or environmental enforcement action). It may also lead to the Procurator Fiscal deciding not to prosecute a case where there has been a breach of criminal law, or in the case subsequently failing because the court funds that the evidence is inadmissible.

2.4 Apart from the use of information in any legal proceedings, the Council could also be open to legal challenge by individuals who claim the Council has justifiably interfered with their right to privacy.

3 Scope of the procedure

3.1 This policy and procedure applies in all cases where either:

- "directed surveillance" is being planned or carried out; or
- the conduct of a CHIS or the use of such a source is being planned or is in operation.

3.2 RIPSA also applies to "intrusive surveillance". Only the Chief Constable of Police Scotland can authorise such surveillance. The Council does **not** have the power to undertake intrusive surveillance. The use of a surveillance device *inside* residential premises or a vehicle is intrusive surveillance.

Examples of intrusive surveillance might include a camera placed in a care home for the purpose of investigating thefts of service users' property, or a camera placed on one Council tenancy to monitor activities inside another tenancy.

The Council should **not** undertake activities of this nature.

3.3 The use of surveillance devices outside residential premises or a vehicle, directed to what is going on inside the premises/vehicle is not intrusive, unless the device consistently provides information of the same quality and detail as might be expected from a device inside the premises/vehicle. The sort of surveillance undertaken by the Council is unlikely to reach this level of sophistication, but if officers are in any doubt, they should consult with their line manager and seek legal advice if appropriate. As technology improves, it will be necessary to keep the Council's activities under review.

Examples of non-intrusive surveillance include the use of a CCTV camera in the street to monitor antisocial behaviour, or at a site where fly-tipping is known to take place.

Monitoring the level of noise generated by an antisocial tenant (but not the actual words) is also unlikely to be classed as intrusive and so can be lawfully carried out by the Council (subject to appropriate authorisation if classed as directed surveillance).

3.4 Devices carried into a home or private vehicle by a CHIS do **not** amount to intrusive surveillance, as long as the source has been invited in. However, the device must not be left behind when the source leaves the premises or vehicle.

3.5 Directed surveillance broadly means watching people otherwise than inside their homes or private vehicles, without them being aware that they are being watched. It is covert surveillance which is not intrusive and which is 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 (whether or not specifically identified for the purposes of the investigation or operation). Private information means information about a person's private or family life. If an operation is neither intended nor likely to result in the Council obtaining private information, then it will not be necessary to apply this policy.

3.6 The procedure does not apply to observations that are not carried out covertly, or to unplanned observations made as an immediate response to events, where it would not have been reasonably practicable for an authorisation under the Act to be sought beforehand. For example, it would not apply to the use of overt CCTV systems with appropriate signage, unless cameras were being used in a covert and pre-planned manner as part of a specific operation or investigation targeted against specific individuals, in which case authorisation may be needed. In cases of doubt, the authorisation procedures described below should be followed.

Examples of directed surveillance include:

- hiding a camera in a community centre to find out who has been stealing money;
- using Council officers to monitor the comings and goings at a particular address, e.g. to establish a pattern of occupancy to determine whether or not there has been Council tax fraud, or to investigate whether someone is using their home for business purposes;
- using private investigators to monitor antisocial behaviour at a Council tenancy; or
- asking a member of the public to maintain a log of all visitors to a neighbouring property.

3.7 However, directed surveillance does **not** include the monitoring of noise levels using recording equipment. The Code of Practice suggests that even covert recording of suspected noise nuisance does not fall within the scope of RIPSA or this policy, provided that the intention is only to record excessive noise levels from adjoining premises and the recording device is calibrated to record only excessive noise levels.

3.8 One area of particular interest to the regulator at present is the use of the internet, including **social media,** by local authorities for investigative purposes. The need for, or at the very least the advisability of obtaining, RIPSA authorisation for activities conducted on social networking sites has been highlighted in a number of annual reports by the regulator. Council officers must be aware that just because individuals are putting personal information about themselves in the public domain does not mean that it is fair game. If Council staff are repeatedly viewing a person's Facebook or other social media websites for the purpose of intelligence gathering and data collation, they must seek the appropriate authorisation under this policy. Paragraphs 3.11 to 3.16 of the Covert Surveillance and Property Interference Code sets out useful guidance on use of the internet for surveillance, including the use of social networking sites.

Examples

Housing Benefit

The Housing Benefits team may want to access a person's social media profile to find out how much time they were spending at their Council tenancy. They might have suspicions that the person was spending a large portion of their time living abroad. Regularly accessing the person's Facebook page could be a helpful way to investigate this. However, they must ensure that such activity was properly authorised in accordance with the procedures described below.

Social Work

A social worker in criminal justice may want to monitor an offender's behaviour online to ensure he is adhering to the terms of a court order (eg by staying in the Falkirk area). Even if the offender posts publicly on social media about his whereabouts, regular viewing of his social media activities is directed surveillance and must be authorised in accordance with the procedures described below.

3.9 A <u>covert human intelligence source</u> is a person who establishes or maintains a personal or other relationship with another person for the covert purpose of:

(a) obtaining information or the providing of access to any information; or

(b) disclosing information obtained by the use of or as a consequence of that relationship.

The term covert human intelligence source includes undercover officers, informants and agents. It might also cover people used to make test purchases, including the Council's own trading standards officers. However, the definition of a CHIS requires there to be an established relationship. This takes many test purchasing operations outwith the scope of RIPSA and this procedure, as the carrying out of an everyday transaction does not of itself establish a relationship. Nor will asking a concerned citizen to "keep an eye on" suspicious behaviour by itself amount to source activity (although it may be directed surveillance conducted on behalf of the Council). When members of the public are volunteering information about incidents witnessed in their neighbourhood (such as antisocial behaviour or alleged breaches of planning control), they would not be regarded as a CHIS.

Examples of circumstances in which the Council might use CHIS include:

- using an undercover trading standards officer to ascertain from a seller of goods the details of the supplier of counterfeit products; or

- engaging a juvenile to establish a relationship with a local shopkeeper, in order to attempt to make a test purchase of alcohol.

The comments made about use of the internet for directed surveillance in paragraph 3.8 are relevant also to CHIS. For example, a trading standards officer may want to attempt to make a test purchase from an online seller (eg on eBay or Gumtree), following a report of counterfeit goods. If that officer enters into a series of online communications with the seller prior to the purchase, that may be considered an “established relationship” with amounts of CHIS.

3.10 The covert exploitation of a relationship is arguably a greater interference with a person’s privacy than directed surveillance. The use of a source may also expose the source to serious danger. For these reasons, the use of a CHIS by the Council is discouraged and should be seen as an absolute last resort. It is expected that officers who are considering the use of a CHIS will have fully considered alternative approaches.

4 Principles of surveillance

4.1 In planning and carrying out directed surveillance or using or conducting CHIS, Council employees must comply with the following principles:

4.2 Lawful purposes – directed surveillance or CHIS operations must only be carried out where they are necessary to achieve one or more of the permitted purposes set out in RIPSA. The activities must be:

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

(ii) in the interests of public safety; and

(iii) for the purpose of protecting public health.

4.3 Council officers should apply the following criteria when applying for or acting under authorisations:

- Necessity – directed surveillance / CHIS operations must only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

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

- Effectiveness – planned directed surveillance / CHIS operations must only be undertaken by suitably trained or experienced employees, or under their direct supervision. The Council should also consider whether it is the most appropriate agency to be carrying out the investigation. Where it is suspected that a crime such as theft is being committed, the Council should in the first instance inform the police.

- Proportionality – the use and extent of directed surveillance / a CHIS must not be excessive, i.e. the methods of surveillance used must not be more intrusive than is warranted by the seriousness of the activity under investigation. The surveillance should not go beyond the minimum necessary to fulfil the purpose of the surveillance. More detailed guidance on proportionality is given below.

- Collateral intrusion – reasonable steps must be taken to minimise the infringement of privacy of individuals who are not the subjects of the investigation or covered by the authorisation in some other way. Council officers should minimise the scope for acquiring information that is not directly necessary for the investigation being carried out. Where it is likely that there will be collateral intrusion, the applicant must specify this in the application form and explain how this will be managed. Information obtained as a result of collateral intrusion must be disclosed to the Authorising Officer. The Authorising Officer must review the material and order the destruction of anything irrelevant to the investigation.

- Security and welfare – a CHIS authorisation cannot be granted unless arrangements exist providing for:

  (i) an officer of the Council to deal with the CHIS day-to-day (including dealing with the source's security and welfare);

  (ii) a different officer to have a general oversight of the use of the source; and

  (iii) an officer of the Council to have responsibility for maintaining a record of the use made of the source (and maintaining the security of the records – see below).

- Authorisation – all directed surveillance must be authorised in accordance with the procedures described below. There are separate procedures applying to the authorisation of directed surveillance and the conduct of a CHIS. Where both are proposed, separate applications must be completed and submitted, and distinct authorisations will be granted if appropriate. Officers must take care to ensure that they have completed the appropriate application form and the Authorising Officer should reject applications that have not been completed in full, or where the wrong form has been used.

4.4 Council employees carrying out surveillance or CHIS activities **must not** cause damage to any property or harass any person. Authorisation or use or conduct of a CHIS does not amount to a licence to commit a crime. Any Council officer or source who acts beyond acceptable limits will not be protected from prosecution on the basis of the authorisation.

4.5 Council employees carrying out surveillance of CHIS activities should also be aware of any particular sensitivities in the local community where the CHIS is being used and of similar activities being undertaken by other public authorities which could have an impact on the deployment of a CHIS. Officers should take account of any potential adverse impact on community confidence or safety that may result from the use or conduct of a CHIS or use of information obtained from the CHIS. There may need to be consultation with other public authorities in the area to gauge community interest.

5 Proportionality

5.1 Proportionality is a legal principle which arises when considering human rights. It is intended to ensure that measures taken by public authorities which impact on the fundamental rights of citizens are kept within proper limits. Even if there is arguably no breach of human rights legislation, RIPSA itself lays down specific criteria and procedures which require an assessment of proportionality.

5.2 Rights may lawfully be interfered with if there is a recognised legitimate aim pursued by the public authority, in this case the Council. However, the principle of proportionality means that if the same end can be achieved through less intrusion on people's rights (or none at all) then that less intrusive approach should be followed. There should also be a correlation between the importance of the aim pursued and the degree of intrusion into people's rights.

> For example, if the local authority suspected that a person was lying about their address in order to fall within the catchment area for their desired school, surveillance is unlikely to be a necessary or proportionate way in which to investigate the matter. Less intrusive, overt, means such as unscheduled visits to the address in question to obtain the information needed are likely to be more appropriate and should be considered first.
>
> On the other hand, directed surveillance might be more proportionate as a means to detect a fraudulent claim for housing benefit which could cost the Council thousands of pounds.

5.3 Covert surveillance by any means involves a potentially serious breach of individuals' rights to privacy. The Council will therefore need compelling reasons to justify cover surveillance, particularly if the surveillance is to last for an extended period of time.

5.4 Council employees must bear in mind the seriousness of the behaviour which is to be investigated. Potentially serious criminal conduct will be at the higher end of the scale and will justify greater interference. However, even if the offences would only attract a low level of penalty (such as a small fine), the purpose behind the legislation creating the offence may be very serious. For example, trading standards legislation is designed to prevent the sale of dangerous goods or contaminated food, and licensing laws exist to ensure the safety of licensing premises. Another factor that ought to be considered is the impact of the behaviour on other people, both in terms of the gravity and the number of people affected.

6 Authorisation process – general

6.1 Authorisation is required for directed surveillance or the use or conduct of a CHIS. Before applying for authorisation, officers should ensure they have read this policy fully, together with the relevant Code of Practice.

6.2 If there is any uncertainty about whether authorisation is needed or if it is likely to be granted, officers may wish to refer to the flowchart set out in the appendix to this policy. However, 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.

6.3 Authorisation is needed 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.

6.4 Legal advice may be obtained from the Council's internal Legal team. This is a resource that you are encouraged to access when you have unanswered questions or are looking for some reassurance that you are going about things in the right way.

6.5 Before asking for authorisation, the Council officer who will apply for authorisation must first seek prior approval from their line manager. If this cannot be done, it will be necessary to provide an explanation to the Authorising Officer.

6.6 In terms of the Regulation of Investigatory Powers (Prescription of Officers, Ranks and Positions) (Scotland) Order 2000, authorisations for directed surveillance or the conduct or use of a CHIS can be granted only by Assistant Heads of Service or Investigation Managers and by any officer senior to these positions.

6.7 In Falkirk Council, authorisation can only be granted by a Designated Authorising Officer as set out in the Appendix to this policy. Wherever possible, authorisations shall only be granted by Authorising Officers in a different service to the service seeking the authorisation. All Designated Authorising Officers must undertake training before hearing/granting any applications

6.8 Authorising Officers must not authorise their own activities, i.e. those operations they are directly involved in.

6.9 Authorisations must be given in writing by the Authorising Officer. Forms for the application, review, renewal and cancellation of both directed surveillance and the use or conduct of a CHIS are detailed in section 10 below. However, in urgent cases, authorisation may be given orally. In such cases, a statement that the Authorising Officer has expressly authorised the activity should be recorded in writing by the authorising officer as soon as is reasonably practicable.

6.10 Applications which identify a significant risk of accessing confidential information (see below) can only be authorised by the Chief Executive.

6.11 The role of the Authorising Officer is to ensure that the applicant officer:

- has correctly identified a lawful purpose (see above) 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 the permissible limits of directed surveillance / the conduct of a CHIS; and
- has correctly applied the proportionality test.

<u>Only if the Authorising Officer is actively satisfied on these points should the authorisation be granted.</u>

6.12 Authorising Officers may be required by the IPCO to justify their decision to grant a particular request. It is important that authorisations are not simply signed off automatically. Evidence of a reasoned refusal of request is also vital in evidencing compliance with the law. If evidence obtained by surveillance is used in court, the authorising officer may be called upon to justify the grant of the authorisations.

6.13 Applicants for authorisations and operational staff must see a copy of the authorisation once granted so they are in no doubt as to what the authorisation permits (and make a record or note they have done so).

7 Authorisation process – specific considerations for directed surveillance (period of effect)

7.1 Authorisations given in writing have legal effect for a period of **three months**. An urgent oral authorisation has legal effect for a period of **seventy-two hours**. These periods can be extended by renewal.

8 Authorisation process – specific considerations for CHIS (including period of effect)

8.1 Both the conduct and the use of CHIS require prior authorisation. However, both may be authorised through a single application, as long as care is taken to ensure that the authorisation complies with both procedures.

8.2 A CHIS wearing or carrying a surveillance device does not need a separate directed surveillance authorisation, provided the device will only be used in the presence of the CHIS. If the surveillance device is to be used other than in the presence of the CHIS, a directed surveillance authorisation must be obtained where appropriate.

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

8.4 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.

8.5 There are specific requirements in the case of juveniles (persons under 18):

- only the Chief Executive can authorise such a person to be used as a CHIS or to conduct themselves as such;
- a child under 16 cannot be used where the relationship to which the use of the source would relate is with the child's parent or someone having parental responsibility for the child;
- where a child under 16 is used, an appropriate adult must be present at all meetings with relevant Council officers;
- where a source is under 18, there must be a risk assessment as to both the possibility of physical injury and the possibility of psychological distress and the justification for the authorisation must be considered in light of that assessed risk; and
- reference should be made to the Regulation of Investigatory Powers (Juveniles) (Scotland) Order 2002.

8.6 An urgent oral authorisation lasts for **seventy-two hours**. An authorisation given in writing has legal effect for **12 months**. If the source is under the age of 18 years, the authorisation given in writing has effect for **one month**. These periods can be extended by renewal.

8.7 The Authorising Officer must satisfy himself that appropriate arrangements are in force for the use or conduct of a CHIS. These arrangements must ensure that:

(i) there is a person within the Council who will have day-to-day responsibility for dealing with the source, directing the source's activities, recording any information supplied by the source and for the security and welfare of the source (known as the "**handler**");

(ii) there is another person within the Council who will have general oversight of the use made of the source (known as the "**controller**" – this person must be more senior than the handler);

(iii) there is a person within the Council (who might be the handler or the authorising officer) who will have responsibility for maintaining a record of the use made of the source;

(iv) the records relating to the source will always contain such information as may be required by the Regulation of Investigatory Powers (Source Records) (Scotland) Act 2002 and any regulations made by the Scottish Ministers; and

(v) records which disclose the identity of the source will not be available to persons except where there is a need for access to be made available to those persons.

8.8 Records to be maintained include:

- the identity of the source;
- the identify, where known, used by the source;
- any relevant investigating authority, other than the Council (e.g. police, SEPA);
- the means by which the source is referred to within each relevant investigating authority (i.e. any code names);
- any other significant information connected with the security and welfare of the source;
- any confirmation made by the authorising officer when 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 handler and controller of the source and (if different) the person responsible for maintaining a record of the use made of the source;
- the periods during which those persons have discharged their responsibilities;
- the tasks given to the source and the demands of him/her in relation to their activities as a source;
- all contacts or communications between the source and any officer of the Council;
- the information obtained by the conduct or use of the source;
- any dissemination by the Council of information obtained in that way;

- (where the source is not an undercover officer of the Council) any payment, benefit or reward and every offer of a payment, benefit or reward that is made by or on behalf of the Council in respect of the source's activities;

- any risk assessment made in relation to the source;

- the circumstances in which tasks where given to the source; and

- the value of the source to the Council.

9 Review process

9.1 All authorisations legally extant must be reviewed by an Authorising Officer **within six weeks** of being granted. Authorising Officers are, however, encouraged to consider review of authorisations after the shortest period possible commensurate with the effectiveness of the operation/investigation. The purpose of the review is to monitor the effectiveness of the surveillance and its continued necessity and proportionality.

10 Renewals and cancellations

10.1 If it is thought necessary for the authorisation to continue beyond the initial period authorised, a renewal application should be submitted shortly before the original authorisation ceases to have effect.

10.2 Authorisations may be renewed by an Authorising Officer <u>at any time before the original has ceased to have legal effect</u>. If not renewed, the authorisation ceases to have effect. Any activities undertaken after that point would not be properly authorised.

10.3 The Authorising Officer must apply to the application the same criteria as justified the original authorisation. The whole circumstances of the case must be fully considered in terms of RIPSA, this procedure and the relevant Code of Practice. Any risk assessment must also be reviewed.

10.4 Authorisations may be renewed on more than one occasion and will have effect for the same period as the original authorisation.

10.5 Before renewing authorisation for the conduct or use of a CHIS, the Authorising Officer must be satisfied that a review has been carried out of the use made of the source, the tasks given to the source and the information obtained from the conduct or use of the source and consider the results of the review.

10.6 The Authorising Officer must cancel any authorisation as soon as he/she is satisfied that it no longer meets the criteria for authorisation. The Authorising Officer will then check the arrangements in place to terminate the surveillance and the handler will advise the source (if any) involved in the operation.

11 Documents / forms

11.1 Directed Surveillance – Written Authorisation: This application must be completed by the applicant officer in all cases not covered by oral authorisation (below). The authorisation section must be completed by the Authorising Officer. It is effective from the time that approval is given.

11.2 Directed Surveillance - Oral Authorisation: This is a record of oral authorisation. When urgent oral authorisation has been sought, the Authorising Officer must make a record of the oral authorisation given as soon as practicable thereafter. Oral authorisation should only be used in cases where the urgency of the situation makes the submission of a written application impractical (but application officers should also consider whether section 1(2)(c) of RIPSA applies – immediate response to events does not require authorisation). This procedure should not be used where the need for authorisation has been neglected or the urgency is of the applicant or Authorising Officer's own making.

11.3 Directed surveillance – Renewal of Authorisation: The application section should be completed by the applicant in all cases where surveillance is required beyond the previously authorised period (including previous renewals). Renewal authorisation must be obtained before the expiry of the original authorised period if the operation is not to cease pending the processing of the renewal application. Again, the renewal of authorisation must be completed by the Authorising Officer.

11.4 Directed surveillance – Cancellation: This form should be completed by the Authorising Officer when the authorisation ceases to be either necessary or appropriate.

11.5 Covert Human Intelligence Source – Application for Authorisation: This should be completed by the applicant officer when seeking to use a CHIS (unless it is a case where oral authorisation has been sought and obtained). If granted, it will be countersigned by the Authorising Officer. It is effective from the time approval is given. A separate application will not be required each time the source is given a new assignment, provided the application specifies the task in broad enough terms to cover each assignment. If the nature of the assignment changes, however, the existing authorisation should be cancelled and a new application for authorisation submitted.

11.6 Covert Human Intelligence Source – Record of Oral Authorisation: Oral authorisations for the use or conduct of a CHIS are **expressly discouraged**. In emergency circumstances where these are required, the Authorising Officer must make a record of the authorisation given as soon as practicable. The record should make clear that an oral authorisation has preceded the completion of the form and that fact and the particular emergency circumstances must be fully recorded on the form. This procedure should not be used where the need for authorisation has been neglected or where the emergency is of the applicant or Authorising Officer's own making.

11.7 Covert Human Intelligence Source – Renewal of Authorisation: The application section should be completed by the applicant in all cases where conduct or use of the source is required beyond the previously authorised period (including previous renewals). The renewal of authorisation section should be completed by the Authorising Officer. Renewal authorisation must be obtained before expiry of the original authorised period if the operation is not to cease pending processing of the renewal application.

11.8 Covert Human Intelligence Source – Cancellation of Authorisation: This should be completed by the Authorising Officer when the authorisation ceases to be either necessary or appropriate. An Authorising Officer who has granted or renewed an authorisation for a CHIS must cancel it if authorised use or conduct no longer satisfies the criteria applying to its grant or renewal (i.e. the conduct is no longer necessary or proportionate or security/welfare/handling etc. arrangements no longer exist). In these circumstances, the authorising officer should not await an application to cancel, but must take the initiative him/herself.

12 Security and retention of documents

12.1 Documents created under this procedure are highly confidential and must be treated as such. Services must make proper arrangements for their retention, security and destruction, in accordance with the requirements of Data Protection Legislation as defined by the Data Protection Act 2018 and the Codes of Practice.

12.2 All applications must be retained – both those granted and those refused. The Codes of Practice recommend retention of RIPSA records for a period of **at least three years** from the cessation of the authorisation. As the applications will likely contain information of a sensitive nature, officers should ensure that it is kept properly secure.

12.3 Documents will be inspected periodically by the IPCO which has statutory powers of inspection. No records should be destroyed until after they have been inspected by the IPCO.

12.4 The Monitoring Officer (Chief Governance Officer) must maintain a register of all current and past authorisations. Authorising Officers must ensure that sufficient records (of authorisations, renewals, cancellations and oral authorisations) are provided to keep this up-to-date. Information which must be provided to the Monitoring Officer includes:

- a copy of the application and authorisation, together with any supporting documentation and notification of the approval given by the authorising officer;
- a copy of any application for renewal, together with the supporting documentation submitted when the renewal was requested;
- the results of any reviews carried out by the authorising officer, including any cancellations and the reasons for those;
- the reasons, if any for refusing authorisation or refusing an application for renewal; and
- the date and time when any instruction was given by the authorising officer to cease using a CHIS.

13 Data protection

13.1 Any evidence obtained through surveillance activities will in most cases constitute personal data for the purposes of the Data Protection Legislation. This requires that personal data should (amongst other things) be adequate, relevant, accurate, up-to-date, not excessive and kept secure.

13.2 In relation to the relevance requirement, the Codes of Practice recommend that material acquired through collateral intrusion should be removed from files. However, Council officers must be careful to avoid endangering the evidential value of any material recovered before destroying any parts of it.

13.3 Data subjects have a right to request personal data held about them. A request for access to material acquired through surveillance should be handled under the Council's normal subject access request procedures. In many cases, this may mean that access to the information is refused on the ground of possible prejudice to the prosecution of an offence, but this must be assessed on a case-by-case basis.

14 Confidential information

14.1 RIPSA does not provide any special protection for confidential information, but it does require 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.

14.2 Confidential information includes:

- information subject to legal privilege (which attaches to most communications between a professional legal adviser and a client);
- confidential personal information (information held in confidence relating to the physical or mental health or spiritual counselling of a person); and
- confidential journalistic material (created for journalism but supplied subject to an undertaking to hold it in confidence).

14.3 Legal advice should be obtained if any of these types of confidential information are likely to be involved in an operation.

15 Surveillance activities by other public authorities

15.1 Council officers may be asked to assist in surveillance operations being conducted by other public authorities, such as the police, the Benefits Agency, or HMRC. In such cases, it is for the organisation seeking assistance from the Council to ensure that it has appropriate authorisations in place. Council officers should ask to see those authorisations, or at least written confirmation that they have been granted.

15.2 If the Council is acting jointly with another body, but carrying out its own surveillance activities, the Council should have its own authorisations in place.

16 Complaints

16.1 Any person who is aggrieved by any conduct which falls within the scope of this procedure is entitled to complain to the Investigatory Powers Tribunal online at https://www.ipt-uk.com/ or, at the following address:

Investigatory Powers Tribunal
PO Box 33220
LONDON
SW1H 9ZQ

16.2 The Tribunal has power to award compensation where there has been a failure to following the appropriate procedures under RIPSA and can make any other order it thinks fit, including orders quashing any grant of authorisation and requiring the destruction of records obtained.

16.3 Complaints may also be directed via the Council's internal complaints procedure.

Version Number	Purpose/Change	Author	Date
1.00	Approved by Executive	Chief Governance Officer	November 2015
2.00	Updated for Data Protection 2018 Approved by Information Governance Manager	Information Governance Manager	28.06.18
3.00	Updated references to Codes of Practice Reduction in number of Authorising Officers Approved by Information Management Working Group	Information Governance Manager	22.11.18
4.00	Updated in light in 2018 inspection report	Information Governance Manager	14.3.19

DESIGNATED AUTHORISING OFFICERS

Chief Executive

Chief Governance Officer

CHILDRENS SERVICES

Head of Education

Head of Social Work Children's Services

COPORATE AND HOUSING SERVICES

Strategy and Private Sector Manager

Internal Audit Manager

DEVELOPMENT SERVICES

Head of Planning and Economic Development

Head of Environmental Services