<table>
<thead>
<tr>
<th>Version Control</th>
<th>Comments</th>
</tr>
</thead>
<tbody>
<tr>
<td>V1 Sept 2014</td>
<td>Approved by Audit Committee on 4 September 2014 following implementation of recommendations of the OSC Inspection Report dated 7 February 2013</td>
</tr>
<tr>
<td>V2 May 2016</td>
<td>Subject to approval by Audit Committee on 26 May 2016 following implementation of recommendations of the OSC Inspection Report dated 24 November 2015</td>
</tr>
</tbody>
</table>

To be approved by Audit Committee 26 May 2016
# TABLE OF CONTENTS

1. BACKGROUND AND POLICY
   1.1. Introduction
   1.2. Objective
   1.3. Scope of the Policy

2. AUTHORISATION PROCEDURE
   2.1. Applications for Authorisations
   2.2. Who can grant Authorisations?
   2.3. Granting of Authorisations
   2.4. Vulnerable Individuals
   2.5. Juveniles
   2.6. Time Periods
   2.7. Refusals of Authorisations
   2.7. Collaborative Working

3. RENEWALS, REVIEWS AND CANCELLATIONS
   3.1. Renewals
   3.2. Reviews
   3.3. Cancellation

4. ENSURING COMPLIANCE WITH RIPSA
   4.1. Senior Responsible Officer
   4.2. Monitoring and Quality Control
   4.3. Oversight
   4.3. Complaints

5. RECORD KEEPING AND SECURITY
   5.1. Central Record of Authorisations
   5.2. Retention and Destruction of Documents
   5.3. Data Protection and Information Security

SCHEDULE
   Part 1. Authorising Officers
   Part 2. Training Plan
1. BACKGROUND AND POLICYdirected

1.1. Introduction

1.1.1. Stirling Council is a public authority for the purposes of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) and as such has powers in certain limited circumstances to authorise directed covert surveillance and the use of covert human intelligence sources (“CHIS”).

1.1.2. In some circumstances, it may be necessary for Stirling Council employees, in the course of their employment, to make observations of a person in a covert manner i.e. without that person’s knowledge. By their very nature, actions of this sort may constitute an interference with that person’s right to privacy and may give rise to legal challenge as a potential breach of Article 8 (right to respect for private and family life) or Article 6 (right to a fair trial) of the European Convention of Human Rights (“the ECHR”).

1.1.3. Covert activities will be lawful if the activities are authorised in accordance with RIPSA and if they are conducted in line with the terms of the authorisation.

1.2. Objective

1.2.1. The objective of this policy is to ensure that all directed covert surveillance and all use of CHIS carried out by Stirling Council is carried out lawfully. It should be read in conjunction with the Regulation of Investigatory Powers (Scotland) Act 20001 (“the Act”) and the Code of Practice on Covert Surveillance and Property Interference dated November 2014 (“The Covert Surveillance Code of Practice”) and the Code of Practice on Covert Human Intelligence Sources also dated November 2014 (“The CHIS Code of Practice”) both issued by the Scottish Ministers2. The Office of the Surveillance Commissioners Procedures and Guidance dated December 2014 (“the OSC Procedures and Guidance) is also a useful source document.

1.2.2. Where procedures set out in this policy are not followed, evidence acquired will be unlawful and inadmissible in Court. Stirling Council may also be open to legal action for a breach of ECHR or a complaint to the Investigatory Powers Tribunal set up under the Regulation of Investigatory Powers Act 2000 (“the UK Act”).

1.3. Scope of the Policy

1.3.1. This policy applies in cases where covert surveillance or the use of CHIS is being planned.

1.3.2. Authorising Officers will not be able to authorise an application for authorisation prior to first having attended the appropriate RIPSA Authorising Officer Training as provided for in the Training Plan annexed at the Schedule Part 2.

1.3.3. No Officer will be able to make an application for authorisation or carry out surveillance prior to first having attended appropriate RIPSA Applicant Training as provided for in the Training Plan annexed at the Schedule Part 2.

1.3.4. Directed surveillance is defined in The Covert Surveillance Code of Practice as surveillance undertaken ‘for the purpose of a specific investigation or operation’ and ‘in such a manner as is likely to result in the obtaining of private information about a person’. The surveillance must

1 The text of the Act can be accessed on the UK Statute Law Database at http://www.statutelaw.gov.uk/legResults.aspx?LegType=All+Legislation&title=regulation+investigatory+scotland&Year=2000&searchEnacted=0&extentMatchOnly=0&confersPower=0&blanketAmendment=0&type=QS&NavFrom=0&activeTextDocId=115588&PageNumber=1&SortAlpha=0

also be covert i.e. conducted in such a manner as is calculated to ensure that the persons subject to surveillance are unaware that it is taking place.

1.3.5. Private Information includes information about a person’s private and family life, their home and their correspondence. The fact that a covert surveillance operation may take place in a public place (or on business premises) does not mean that it cannot result in the collecting of private information about an individual. The concept of private life is broadly interpreted and includes not only personal information but also information about an individual’s relationships with others and may include how he runs his business and professional affairs. Prolonged surveillance targeting of an individual will, almost without exception, result in the obtaining of private information about the individual and potentially others that they come into contact with. Family life is treated as extending beyond the formal relationship created by marriage. The key issue is likely to be whether there is a reasonable expectation of privacy in the circumstances. If there may be, the safest option is to apply for an authorisation.

1.3.6. Surveillance includes:
- Monitoring, observing or listening to persons, their movements, their conversation or their other activities or communications;
- Recording anything that is monitored, observed or listened to in the course of surveillance;
- Surveillance by or with the assistance of a surveillance device.

1.3.7. Surveillance can be overt or covert. Authorisation is only required for covert surveillance. Overt surveillance is where it is carried out in a manner that anyone subject to it is aware that it is taking place and may include:
- City Warden observations in the community as their presence will be obvious due to their uniforms; and
- Closed Circuit Television installations (“CCTV”) which are plainly visible and where appropriate signs are displayed advising of the presence of the CCTV.
Covert surveillance is where it is carried out in a manner that anyone subject to it is not aware that it is taking place and may include:
- The use of CCTV for a specific covert operation;
- Covert monitoring of the social media accounts of an individual.

1.3.8. The following do not amount to directed surveillance:
- Observations which are carried out overtly;
- Casual, unplanned and ad-hoc covert observations that do not involve the systematic surveillance of specific persons for a specific operation or investigation. However if the evidence obtained is to be able to stand up to scrutiny the fact that it was obtained from a casual unplanned, ad hoc observation should be well documented; and
- Unplanned observations made as an immediate response to events where it was not reasonably practicable to obtain an authorisation e.g. observations of a suspicious person by a police officer on patrol.

1.3.9. An application for directed surveillance must be submitted for all under-age sales operations. This is required even if covert recording equipment is not worn by the test purchaser because the adult trading standards or other officer present and observing the under-age sales operation will be considered to have obtained private information. This is because the ECHR has construed the manner in which a business is run to fall within the scope of the definition of private information. It will be appropriate to combine multiple under-age sales operations within a single application only where the intelligence is sufficient to prevent a ‘fishing expedition’.

1.3.10. This policy does not apply to any disciplinary investigation or activity involving the surveillance of employees of the Council, unless such surveillance directly relates to a regulatory function of the Council.
1.3.11. This policy does not apply to CCTV which are plainly visible and where appropriate signs are displayed advising of the presence of the CCTV. It does however apply to the use of CCTV for directed surveillance. If an operator of any Stirling Council CCTV is approached by anyone requesting that the operator undertake directed surveillance then the operator must, prior to complying with any such request, obtain a written copy of the authorisation. The authorisation must detail the use of a specific CCTV for the purpose of directed surveillance and be signed by a Stirling Council Authorising Officer or, in the case of a Police Scotland authorisation, by an officer of at least the rank of Superintendent. In urgent cases an authorisation approved by a Police Officer of at least the rank of Inspector may be acceptable. A copy should be kept and the original forwarded to the Solicitor to the Council for recording in the Central Record of Authorisations. If an Officer is unsure about an aspect of this procedure they should refer the matter to their line manager or the Solicitor to the Council.

1.3.12. When operating in an online environment the same considerations apply when assessing whether an application for directed surveillance or the use of a CHIS is required. As the OSC Procedures and Guidance states at paragraph 288 “The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation.” It goes on to highlight that whilst it is the responsibility of an individual to set privacy settings in Social Networking Sites (“SNSs”) in such a way to prevent unsolicited access to private information that where this setting is not applied an officer cannot assume that the information is no longer private information and is instead ‘open source’. Whereas overt monitoring of a social media profile in a SNS e.g. via the Council’s Facebook page will be unlikely to initially amount to directed surveillance, repeat visits to the same SNS may develop into directed surveillance and this must be considered on a case by case basis. By contrast, covert monitoring of a social media profile by using a false identity will be covert but may still be lawful and as such would require an authorisation for directed surveillance. It is not anticipated that Stirling Council staff will set up a false identity for this purpose. Similarly, when visiting a SNS or website where interaction with others takes place, opposed to online research and general observations, authorisation for the use of a CHIS may be required. All officers need to be alert to this when carrying out their daily activities. Further Guidance and Training on this subject will be produced as both professional practice and the law in this area develops.

1.3.13. A CHIS is defined in the CHIS Code of Practice as someone who establishes or maintains a relationship with another person with the intention of covertly obtaining information from that person. Information is obtained covertly where it is done in a manner calculated to ensure that other person is unaware that it is happening.

1.3.14. The following do not amount to the use of a CHIS:-
- Tasks given to persons to ascertain purely factual information e.g. the location of cigarette vending machines in licensed premises;
- Covert test purchase transactions under existing statutory powers where the officers involved do not establish a personal or other relationship for the purposes stated e.g. the purchase of a music CD for subsequent expert examination would not require authorisation but where the intention is to ascertain from the seller where he buys suspected fakes then authorisation should be sought beforehand.

1.3.15. In cases of doubt, the authorisation procedures described below should be followed. Officers are also encouraged to seek advice and guidance from the Solicitor to the Council acting as the Senior Responsible Person and always where a CHIS is to be authorised.

1.3.16. It should be noted that Stirling Council is not authorised to conduct intrusive surveillance under any circumstances. Intrusive surveillance is surveillance in relation to anything taking place in any private vehicle or in any residential premises. Surveillance in common areas such as common stairs and closes is not intrusive. Further, surveillance is not intrusive if it is directed into a home or a private vehicle from outside of that home or vehicle unless the information provided is consistently of the same quality as would be provided by having a device actually present in the home or vehicle.

2. AUTHORISATION PROCEDURE
2.1. Applications for Authorisations

2.1.1. An applicant, who must have attended the RIPSA Applicant Training, who wishes to conduct directed surveillance or use a CHIS must seek and be granted authorisation prior to carrying out the operation. Applications must be made by the applicant on the approved forms only [INSERT NAME OF FORMS – LINK TO SOURCE]. No other style of form may be used. Notification of a pending application must be given by e-mail to the Solicitor to the Council by the applicant and a unique reference number for each application will be allocated by the Solicitor to the Council.

2.2. Who can grant Authorisations?

2.2.1. Only applications for authorisations received on the approved form will be considered and authorised/refused as appropriate by either the Chief Executive or the Director of Housing and Environment or the Director of Corporate Operations, each acting in their capacity as Authorising Officers. The Authorising Officer details are set out in the Schedule Part 1. Authorising Officers are not permitted to delegate this power.

2.2.2. Authorising Officers should avoid authorising their own activities wherever possible although they may do so in exceptional cases.

2.3. Granting of Authorisations

2.3.1. Authorisations must be in writing. In urgent cases it is possible for an authorisation to be granted orally although the authorisation should be recorded in writing as soon as possible thereafter. A case will be regarded as urgent only if the time that would elapse before the Authorising Officer was available to grant the authorisation would be likely to endanger life or jeopardise the investigation. An operation will not be regarded as urgent where the need for an authorisation has been neglected by the applicant or the urgency is of the Authorising Officer's own making.

2.3.2. Authorising Officers should give full details of their reasoning in coming to a decision on each particular application, and should give sufficient comment to establish that they have made themselves fully aware of all relevant factors before coming to that decision.

2.3.3. An Authorising Officer giving an authorisation for the use of directed surveillance or use of a CHIS must be satisfied that:

2.3.3.1 The authorisation is necessary for one or more of the following purposes:-
- for the purpose of preventing or detecting crime or the prevention of disorder,
- in the interests of public safety; or
- for the purpose of protecting public health.

When deciding whether surveillance is ‘necessary’ for any of the above purposes, the Authorising Officer should consider whether there is any other reasonable and effective way of achieving the desired objective.

2.3.3.2 The surveillance is proportionate. There should be a reasonable relationship between the seriousness of the mischief being addressed and the degree of intrusion into people’s lives. If the same end can be reached by less intrusive means, then the less intrusive path should be taken. For criminal offences, the potential punishment by Court e.g. the level of fine, is a useful guide to proportionality but it should be noted that some statutory offences which attract only small fines are designed to prevent potentially life threatening situations e.g. sale of dangerous goods. Such factors weigh in favour of surveillance being proportionate. Other factors which will weigh against
surveillance being proportionate include the possibility of collateral intrusion and the possibility of confidential material being uncovered.

2.3.3 In summary, a consideration of proportionality requires reviewing three elements:-

- that the proposed covert surveillance is proportionate to the mischief under investigation;
- that it is proportionate to the degree of anticipated intrusion on the target and others; and
- it is the only option, other covert means having been considered and discounted.

2.3.4 If the surveillance involves the use of CHIS, satisfactory arrangements must exist for the management of the CHIS. There should at all times be a designated ‘Handler’ with responsibility for the CHIS’s security and welfare. Where an officer is undertaking ‘undercover work’ this should be the CHIS’s line manager. There should also be a designated ‘Controller’ who has oversight of the use made of the CHIS. This would ordinarily be the Handler’s line manager and any such officer must first have received appropriate RIPSA training. The Authorising Officer should be responsible for maintaining a record of the use made of the CHIS.

2.3.5 Authorisation is also required for the use of non-officer CHIS, for example where an officer receives information from someone who approaches them voluntarily on repeated occasions. Care needs to be taken to guard against the risk of a casual informant becoming a CHIS by the inadvertent development of a relationship with a CHIS over a period of time.

2.3.6 The Regulation of Investigatory Powers (Source Records) (Scotland) Regulations 2002 details the particulars which must be included in the records relating to each source and includes:

- The identity of the CHIS and the identity used by the CHIS in the operation;
- The detail of any other relevant investigating authority involved;
- The means by which the CHIS is referred in each investigating authority;
- Any other significant information connected with the security and welfare of the CHIS and confirmation these have been properly explained to and understood by the CHIS;
- The date when and the circumstances in which the CHIS was recruited;
- The identities of the Handler, Controller and Authorising Officers and the period(s) in which these people have discharged their responsibilities;
- All contact/communications between the CHIS and the Handler;
- Information obtained through the conduct or use of the CHIS and any dissemination of that information; and
- Every payment, benefit or reward or offer of these made or provided by or on behalf of any relevant investigating authority in respect of the CHIS’s activities.

2.4. Vulnerable Individuals

2.4.1 Vulnerable individuals, such as the mentally impaired, will only be authorised to act as a CHIS in the most exceptional circumstances. Authorisation by the Chief Executive or, in his absence, the Head of Paid Service deputising for the Chief Executive will be required.

3 **Collateral intrusion** refers to the fact that 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 the risk of collateral intrusion as far as possible.

4 **Confidential material** consists of (1) matter subject to legal privilege e.g. correspondence between a legal advisor and client, (2) confidential personal information e.g. medical files or (3) confidential journalistic materials e.g. material acquired for the purposes of journalism and held subject to an undertaking to hold them in confidence. Operations should be designed to minimise the possibility of confidential material being acquired as far as possible.
2.5. Juveniles

2.5.1. A Juvenile is any person under 18 years of age. The use or conduct of any CHIS under sixteen years of age and living with their parents cannot be authorised for them to give information about their parents or any person who has parental responsibilities in respect of them.

2.5.2. Such CHIS’s can give information about other members of their immediate family in exceptional circumstances. A parent, guardian or other ‘appropriate adult’ should be present at meetings with any juvenile source under 16 years of age.

2.5.3. The authorisation should not be granted unless or until:

- The safety and welfare of any juvenile CHIS has been fully considered;
- The Authorising Officer has satisfied himself/herself that any risk has been properly explained and understood by the juvenile;
- A risk assessment has been undertaken as part of the application to deploy such a CHIS, covering the physical dangers and the moral and psychological aspects of his or her deployment.
- Deployment of a juvenile CHIS will only be authorised by the Chief Executive or, in his absence the Head of Paid Service deputising for the Chief Executive. The maximum duration of such an authorisation is 1 month.

2.6. Time Periods

2.6.1. Urgent oral applications expire after 72 hours (beginning with the time when the authorisation was granted). If required they can be renewed for a further period of 3 months if renewed in writing.

2.6.2. Written authorisations in respect of directed surveillance will expire (unless renewed or cancelled) at the end of a period of 3 months beginning on the day from which they took effect.

2.6.3. Written authorisations in respect of the use of CHIS will expire (unless renewed or cancelled) at the end of a period of 12 months beginning on the day from which they took effect.

2.7. Refusals of Authorisations

2.7.1. The refusal of an application for authorisation shall be noted on the original application.

2.8 Collaborative Working

2.8.1 Where one agency is acting on behalf of another it will normally be the case that the tasking or lead agency shall obtain and provide the authorisation.

3. RENEWALS, REVIEWS AND CANCELLATIONS

3.1. Renewals

3.1.1. At any time before an authorisation would expire (including urgent oral authorisations) the authorisation may be renewed in writing for a further period of 3 months (directed surveillance)/12 months (use of CHIS) beginning with the day on which the previous authorisation cease to have effect. Renewals may also be granted orally in urgent cases and last for a period of 72 hours.

3.1.2. Applications should only be made shortly before the authorisation is due to expire. The tests applicable to renewals are identical to those for initial authorisations. The surveillance or use of CHIS must continue to be necessary and proportionate for a renewal to be granted.
3.1.3. Applications for renewals should be made on form [INSERT NAME OF FORM – LINK TO SOURCE].

3.1.4. Any Authorising Officer may renew an authorisation. They may be renewed more than once, provided they continue to meet the criteria for the authorisation.

3.1.5. Authorisations for the deployment of a juvenile CHIS are renewable for 1 further period of 1 month.

3.2. Reviews

3.2.1. All authorisations must be reviewed by the original Authorising Officer at intervals of not more than 1 month. The Authorising Officer should set an appropriate date for review of each matter based on the nature of the particular operation at the time that the authorisation is granted. Any changes in circumstances must be considered. The review may lead to the authorisation being continued, varied or cancelled. Details of the review and the decision reached shall be noted on form [INSERT NAME OF FORM – LINK TO SOURCE]. Details of the review and the decision reached shall also be noted on the original application.

3.3. Cancellation

3.3.1. An authorisation shall not be permitted to expire; the Authorising Officer must ensure that all authorisations are cancelled as soon as they are no longer required and must cancel an authorisation if he/she is satisfied that the directed surveillance or use of CHIS no longer satisfies the criteria upon which it was authorised. Form [INSERT NAME OF FORM – LINK TO SOURCE] should be used.

4. ENSURING COMPLIANCE WITH RIPSA

4.1. Senior Responsible Officer

4.1.1. The Solicitor to the Council acting as the Senior Responsible officer (“SRO”) is responsible for the oversight of the competence of the Authorising Officers and the operation of the RIPSA processes in use within Stirling Council.

4.1.2. An Annual Report on Stirling Council’s use of RIPSA will be brought to Audit Committee to ensure that the RIPSA Policy and Procedures remains fit for purpose (in accordance with paragraph 3.29 of the Covert Surveillance Code of Practice).

4.2. Monitoring and Quality Control

4.2.1. Each Authorising Officer must maintain a record of all applications for authorisation, including where an application has been refused, renewals, reviews and cancellations. This record must be kept in a secure, locked location. Separate records should be maintained in respect of the authorisation of directed surveillance and the use of CHIS.

4.2.2. All original documentation will be reviewed by Legal Services promptly upon receipt by the Solicitor to the Council, acting as the SRO. The purpose of the review is to identify any areas of procedural or policy weakness and to develop internal training updates, including practice improvement notes to enable more robust and complaint practice.

4.3 Oversight

4.3.1. The Office of Surveillance Commissioners (OSC) provides independent oversight of the use of the powers contained within the Act. This oversight includes inspection visits by Inspectors appointed by the OSC, ordinarily every 3 years.

4.3.2. Any surveillance activity which is not properly authorised must be reported by the SRO to the Chief Surveillance Commissioner at OSC.
4.3. Complaints

4.3.1. The UK Act establishes an independent tribunal called the Investigatory Powers Tribunal. This Tribunal has full powers to investigate and decide any cases within its jurisdiction, which includes Scotland. The Tribunal is a court which investigates and determines complaints of unlawful use of covert techniques by public authorities which infringe on an individual’s right to privacy.

4.3.2. The Stirling Council Complaints procedure [LINK TO Stirling Council Complaints Customer Guide] will also be available for any aggrieved person to make a complaint about the carrying out of covert directed surveillance by the Council.

5. RECORD KEEPING AND SECURITY

5.1. Central Record of Authorisations

5.1.1. The Solicitor to the Council, acting as the RIPSA Coordinating Officer, shall be responsible for the day to day oversight of the Council’s RIPSA activities and the maintenance of the Central Record of Authorisations. Authorising Officers shall notify the Solicitor to the Council of the grant, refusal, renewal or cancellation of any authorisation and the name of the applicant officer within 24 hours of authorisation being granted to ensure the accuracy of the Central Record of Authorisations.

5.1.2. Each Authorising Officer must send the original application for authorisation (including where an application has been refused) renewal, review or cancellation to the Solicitor to the Council for inclusion in the Central Record of Authorisations within 3 days of the date of signature.

5.2. Retention and Destruction of Documents

5.2.1. The Authorising Officer shall retain the copy application forms for at least 1 year after the date of cancellation. The Solicitor to the Council will retain the original application forms for at least 3 years after the date of cancellation.

5.2.2. All information recovered through directed surveillance or the use of a CHIS which is relevant to an investigation shall be retained for at least 3 years after the cancellation of the authorisation. The information should be maintained in such a way as to preserve the confidentiality of the CHIS and the information provided by the CHIS.

5.2.3. Where the product obtained from a CHIS could be relevant to pending or future criminal or civil proceedings it should be retained for a suitable further period of time and its retention reviewed at a future date. All other information shall be destroyed as soon as the operation is cancelled.

5.3. Data Protection and Information Security

5.3.1. Documents and copy and draft documents created under this procedure and information obtained from directed surveillance and the use of CHIS is highly confidential and shall be treated as such. Each Service shall make proper arrangements for the retention, security and destruction of such documents and information, in accordance with the requirements of the Data Protection Act 1998 and both the Covert Surveillance Code of Practice and the CHIS Code of Practice.
## Schedule Part 1

### Authorising Officers

<table>
<thead>
<tr>
<th>Rank</th>
<th>Name</th>
<th>Contact Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chief Executive</td>
<td>Stewart Carruth</td>
<td><a href="mailto:carruths@stirling.gov.uk">carruths@stirling.gov.uk</a> 01786 233010</td>
</tr>
<tr>
<td>Director of Corporate Operations</td>
<td>Gerard O'Sullivan</td>
<td><a href="mailto:osullivang@stirling.gov.uk">osullivang@stirling.gov.uk</a> 01786 233063</td>
</tr>
<tr>
<td>Director of Housing &amp; Environment</td>
<td>Robert Steenson</td>
<td><a href="mailto:steenonr@stirling.gov.uk">steenonr@stirling.gov.uk</a> 01786 233084</td>
</tr>
</tbody>
</table>
Schedule Part 2
Training Plan

Attach a copy of the Training Plan if approved by Audit Committee