Policy and Procedures
Authorisation of the Use of Covert Human Intelligence Source

Regulation of Investigatory Powers (Scotland) Act 2000

1. Background

1.1 The use of people to provide information ('informants') is a valuable resource for the protection of the public and the maintenance of law and order. In order that local authorities and law enforcement agencies are able to discharge their responsibilities, use is made of 'undercover' officers and informants. These are referred to as 'covert human intelligence sources' or 'sources' and the area of work of undercover officers and informants to whom this procedure applies will be referred to as 'source work.'

1.2 Until October 2000 the use of such sources was not subject to statutory control in the UK. From that date a legal framework ensures that the use, deployment, duration and effectiveness of sources is subject to an authorisation, review and cancellation procedure.

2. Dumfries and Galloway Council Policy Statement

2.1 In some circumstances it may be necessary for Dumfries and Galloway Council employees, in the course of their duties, to make use of informants and to conduct operations in a covert manner, i.e. the surveillance is carried out in a manner calculated to ensure that the subject is unaware that it is or may be taking place. By their nature, actions of this sort may constitute an interference with that person's right to respect for privacy and may give rise to legal challenge, for example, as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 ('the right to respect for private and family life, home and correspondence').

2.2 The Regulation of Investigatory Powers Act 2000 (RIPA) and the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) together provide for the first time a legal framework for covert surveillance and the use of covert human intelligence sources by public authorities (including local authorities) and an independent inspection regime to monitor these activities.

2.3 Whilst the Acts do not impose a requirement for local authorities to seek or obtain an authorisation, Dumfries and Galloway Council employees **shall** adhere to the authorisation procedure before using a source or allowing or conducting an undercover operation.

2.4 Local Authorities are not authorised to carry out intrusive surveillance. Accordingly, employees of Dumfries and Galloway Council cannot lawfully carry out intrusive surveillance within the meaning of the Regulation of Investigatory Powers (Scotland) Act 2000.

2.5 Intrusive surveillance is defined as directed surveillance of anything taking place on residential premises or in a private vehicle that involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device capable of providing information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the private vehicle.
See 3.2.9 and 3.2.10 below for the definition of residential premises and private vehicle.

3. Authorisation Procedure: Objective

3.1 The objective of this procedure is to ensure that all work involving the use or conduct of a source by Dumfries and Galloway Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Regulation of Investigatory Powers (Scotland) Act 2000 and the Scottish Ministers' Code of Practice on the Use of Covert Human Intelligence Sources and the Code of Practice on Covert Surveillance. These can be viewed on the Scottish Government's website http://www.gov.scot.uk

3.2 Definitions

3.2.1 Covert human intelligence source means a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that:

(a) covertly uses such a relationship to obtain information or to provide information or to provide access to information to another person; or

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

A relationship is used covertly if, and only if, it is conducted in a manner calculated to ensure that the person is unaware of its purpose.

3.2.2 Directed surveillance is defined in the Code of Practice as surveillance undertaken "for the purposes of a specific investigation or operation" and "in such a manner as is likely to result in the obtaining of private information about a person." For further guidance on this definition see
This details the case C v Police (2006), a decision of the Investigatory Powers Tribunal.

3.2.3 Authorising Officer is the person who is entitled to give an authorisation for the use or conduct of a source in accordance with section 8 of the Regulation of Investigatory Powers (Scotland) Act 2000, and the Regulation of Investigatory Powers (Prescription of Offices etc. and Specification of Public Authorities) (Scotland) Order 2010, as amended by the Regulation of Investigatory Powers (Authorisation of Covert Human Intelligence Sources) (Scotland) Order 2014.

3.2.4 Handler means the person referred to in section 7(6)(a) of the Regulation of Investigatory Powers (Scotland) Act 2000 holding an office or position within the local authority and who will have day to day responsibility for:

- Dealing with the source on behalf of the local authority;
- Directing the day to day activities of the source;
- Recording the information supplied by the source; and
- Monitoring the source's security and welfare.

3.2.5 Controller means the person/the designated managerial officer within the local authority referred to in section 7(6)(b) of the Regulation of Investigatory Powers (Scotland) Act 2000, responsible for the general oversight of the use of the source.

3.2.6 The conduct of a source is action of that source, falling within the terms of the Regulation of Investigatory Powers (Scotland) Act 2000, or action incidental to it.

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

3.2.8 Private information, in relation to a person, includes any information relating to the person's private or family life.

3.2.9 Residential premises means any premises occupied or used, however temporarily for residential purposes or otherwise as living accommodation.

3.2.10 Private vehicle means any vehicle that is used primarily for the private purpose of the person who owns it or of a person otherwise having the right to use it. This does not include a person whose right to use a vehicle derives only from his having paid, or undertaken to pay, for the use of the vehicle and its driver for a particular journey. A vehicle includes any vessel, aircraft or hovercraft.

4. Scope of the Authorisation Procedure

4.1 This procedure applies in all cases where the use of an undercover officer or source is being planned or carried out.

4.2 This procedure does not apply to:

- Sources that provide information on a voluntary basis without being tasked to do so by a public authority. However, if the source is then asked to establish or maintain a relationship then an authorisation may be required.
- Covert test purchase transactions under existing statutory powers where the officers involved do not establish a personal or other relationship for the purposes stated (see definition of a covert human intelligence source). As an example the purchase of suspected counterfeit clothing for subsequent expert examination would not require authorisation but where the intention is to ascertain from the seller where he buys suspected counterfeits, when he takes delivery etc. then authorisation shall be sought beforehand.

- Tasks given to persons (whether that person is an employee of the Council or not) to ascertain purely factual information (for example the details of vehicles stopping outside a property).

In cases of doubt, the authorisation procedures described below should be followed.

5. Principles of use or conduct of covert human intelligence sources

5.1 In planning and carrying out source work, Dumfries and Galloway Council employees shall comply with the following principles.

5.2 Lawful purposes

Source work shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in the Acts) namely:

5.2.1 For the purpose of preventing or detecting crime or the prevention of disorder;

5.2.2 In the interests of public safety;

5.2.3 For the purpose of protecting public health;

5.2.4 For any other purpose prescribed in an order made by the Scottish Ministers.

Employees carrying out source work or using sources must be aware that a source has no licence to commit crime. Any source that acts beyond the acceptable limits of case law in regard to this principle risks prosecution.

5.3 Confidential material

5.3.1 Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of the Chief Executive.

5.3.2 Confidential material consists of:

- Matters subject to legal privilege (for example between professional legal advisor and client),
- Confidential personal information (for example relating to a person's physical or mental health) or
- Confidential journalistic material.

5.4 Vulnerable individuals

5.4.1 Vulnerable individuals, as defined in the Code of Practice, will only be authorised to act as a source in the most exceptional circumstances. Authorisation of the Chief Executive will be required.

5.5 Juvenile sources

5.5.1 A juvenile, as defined in the Code of Practice, can only be authorised if special safeguards are taken. No authorisation shall be granted for the use or conduct of any source under 16 years of age to obtain information about their parents or any person who has parental responsibility for the source. A parent, guardian

or other 'appropriate adult' must be present at meetings with a source under the age of 16 years.

5.5.2 The authorisation shall not be granted unless or until:

- The safety and welfare of the juvenile 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 a juvenile source, covering the physical dangers and the moral and psychological aspects of his or her deployment.

5.5.3 Deployment of juvenile sources shall only be authorised by the Chief Executive.

5.6 Social networking sites

The Office of Surveillance Commissioners procedures and guidance (July 2016) provides guidance on the use of surveillance of this type of site. With reference to expectations of privacy, it may be that repeated viewing of 'open source' sites may constitute covert surveillance and as such an authorisation may be required.

6. The Authorisation Process

6.1 Applications for the use or conduct of a source will be authorised at the level of Investigation Manager or Assistant Head of Service, or above, as prescribed by the Regulation of Investigatory Powers (Prescription of Offices etc. and Specification of Public Authorities) (Scotland) Order 2010. Even in cases of urgency, authorisation by officers of a lower grade is not permitted. The RIPSA monitoring officer, Legal Services, shall keep and maintain a list of authorisers.

6.2 Authorising Officers should not be responsible for authorising investigations or operations in which they are directly involved, although it is recognised that this may sometimes be unavoidable, especially where it is necessary to act urgently. Where an Authorising Officer authorises such an investigation or operation the central record of authorisations should highlight this and it should be brought to the attention of a commissioner or inspector during his next inspection.
An Authorising Officer should not act as a controller or handler of a source. If need be an Authorising Officer from another service could be asked to consider the application to ensure that this does not happen.

6.3 Authorisations shall be in writing. All applications for covert human intelligence source authorisations shall be made on **Form 1** (ref: *RIPSA 1 CHIS authorising form).* The applicant in all cases must complete this. However, in urgent cases an oral authorisation may be given by the Authorising Officer, after assessing the risks for the source in question, and then followed up by written reasons why the authorising officer or officer considered the case to be urgent.
A statement that the Authorising Officer has expressly granted the authorisation should be recorded on the form or, if that is not possible, in the applicant's notebook or

diary. This should be done by the person to whom the Authorising Officer spoke (normally the applicant) but must later be endorsed by the Authorising Officer.

6.4 All applications for covert human intelligence source renewals shall be made on **Form 2** (ref: *RIPSA 2 CHIS renewal form).* The applicant in all cases must complete this where the source work requires to continue beyond the previously authorised period (including previous renewals).

6.5 Where authorisation ceases to be either necessary or appropriate the Authorising Officer or appropriate deputy shall cancel an authorisation using **Form 3** (ref: *RIPSA 3 CHIS cancel form).*

6.6 Regular reviews of authorisations must be undertaken to assess the need for the continued use of the covert human intelligence source. The results of a review must be recorded using **Form 4** (ref: *RIPSA 3 CHIS review form)*

6.7 The Forms and supplementary material are available on the Council Intranet and will be reviewed and maintained by the RIPSA inter service working group as necessary. The Scottish Government's Code of Practice can be accessed at http://www.gov.scot.uk

6.8 Any person giving an authorisation for the use or conduct of a source must be satisfied that the authorisation is for a prescribed **lawful purpose**. (see 5.2) and must consider and be satisfied with the following criteria:

- The purpose for which the CHIS will be tasked or deployed;
- Where a specific investigation or operation is involved, the nature of that investigation or operation;
- The nature of what the CHIS conduct will be;
- The details of any potential collateral intrusion and why the intrusion is justified;
- The details of any confidential information that is likely to be obtained as a consequence of the authorisation;
- The reasons why the authorisation is considered proportionate to what it seeks to achieve; and
- The level of authorisation required (or recommended, where that is different).

6.9 Authorisation of the use of a Covert Human Intelligence Source can only be granted if sufficient arrangements are in place for managing the source's case. The following must be considered:

6.9.1 Tasking – The assignment given to the CHIS. This must be detailed enough but not so narrow that a separate authorisation is required each time the CHIS is tasked. Unforeseen occurrences must be recorded, as must any deviations from the original task so that consideration can be given to the need for a separate authorisation.

6.9.2 Handlers and Controllers – Arrangements must be in place for oversight and management of the CHIS. The 'Handler' will have day to day responsibility for dealing with the CHIS, directing them, recording the information they supply and for monitoring their security and welfare. The Handler will be managed and supervised by a 'Controller', who will also have general oversight in the use of the CHIS.

6.9.3 Joint working – Where more than one public authority benefits from the use of a CHIS then responsibilities and management of the CHIS can be shared. The

Handler and Controller may not be from the same public authority. Arrangements such as this must be documented.

6.9.4 Security and Welfare – The authorising officer must ensure that a risk assessment is carried out prior to tasking and that the handler has considered the ongoing safety and welfare of the CHIS and continues to consider these after the authorisation is cancelled.

6.10 Necessity
Source work shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s).

6.11 Effectiveness
Planned undercover operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

6.12 Proportionality
The use of covert human intelligence sources shall not be excessive i.e. it shall be in proportion to the significance of the matter being investigated.

6.13 Additionally, the Authorising Officer must make an assessment of any risk to a source, their family or associates in carrying out the conduct in the proposed authorisation. This must be recorded on the authorisation form and any renewal form.

6.14 Use of a covert human intelligence source with technical equipment

6.14.1 A covert human intelligence source wearing or carrying a surveillance device and invited into residential premises or a private vehicle does not require separate authorisation to record activity taking place inside the premises or vehicle. Authorisation for the use of that covert human intelligence source may be obtained in the usual way.

6.14.2 Applicants should apply within their own line management structure unless other arrangements have been agreed or it is unreasonable or impractical in the circumstances.

7. Time Periods – Authorisations

7.1 Urgent oral applications cease to have effect after 72 hours. If required they can be renewed for a further period of 12 months if renewed in writing.

7.2 Written authorisations expire 12 months beginning on the day from which they took effect, except in relation to juvenile sources, which last for one month only.

7.3 It is essential to record the date and time the authorisation was granted on the application form.

7.4 The monitoring officer must be provided with a copy of the application form. The original must be kept by the investigatory service.

8. Time Periods – Renewals

8.1 If at any time before an authorisation would expire (including oral authorisations) the Authorising Officer considers it necessary for the authorisation to continue for the purpose for which it was given, it may be renewed in writing on Form 2 for a further period of 12 months beginning with the day on which the previous authorisation ceases to have effect. Applications should only be made shortly before the authorisation is due to expire. The renewal form must be attached to the original application and the monitoring officer must be provided with a copy of the renewal form. Authorisations can be renewed orally in urgent cases but the renewed authorisation will only last for 72 hours.

8.2 Authorisations for the deployment of a juvenile source are only renewable for a period of one month.

8.3 Any person entitled to authorise may renew authorisations. They may be renewed more than once, provided they continue to meet the criteria for authorisation. The Scottish Government's Code of Practice recommends that, where possible, renewals are granted by the original Authorising Officer.

9. Review

9.1 The Authorising Officer shall review all authorisations as frequently as is considered necessary and practicable. This should be more frequent where the surveillance provides access to confidential information or involves collateral intrusion. This should be decided on a case by case basis, taking account of any change in circumstances. All reviews for directed surveillance will be recorded on **Form 4**.

9.2 Details of the review and the decision reached shall be noted on the review form which must be attached to the original application and the monitoring officer must be provided with a copy of the review form.

9.3 Where possible the review should be carried out by the original Authorising Officer.

10. Cancellation

10.1 The Authorising Officer or appropriate deputy must cancel an authorisation if he/she is satisfied that the use or conduct of the source no longer satisfies the criteria for authorisation or that procedures for the management of the source are no longer in place. An authorisation must always be formally cancelled, it must not simply be allowed to lapse. Where possible, and as soon as possible, the source must be informed that the authorisation has been cancelled. All cancellations shall be recorded on Form 3 and the monitoring officer must be provided with a copy of the cancellation form. Where necessary, the safety and welfare of the CHIS must continue to be taken into account after the authorisation has been cancelled.

11. Monitoring

11.1 Each service or discrete location within services must maintain a record of all applications for authorisation (including refusals), renewals, reviews and cancellations.

11.2 Regular operational reviews must be undertaken by services and monitored by the Inter Service Working Group to ensure that, for example, RIPSA training for

appropriate staff takes place. A record of all satisfactory training must be retained.

12. Security and Retention of Documents

12.1 Documents created under this procedure are highly confidential and shall be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 1998 and the Code of Practice.

12.2 Legal Services will maintain the Central Register of Authorisations. Authorising Officers shall notify the Head of Legal and Democratic Services of the grant, renewal, review or cancellation of any authorisations and the name of the Applicant Officer as soon as practicable and in any event within one week to ensure the accuracy of the Central Register. This will be achieved by sending a signed and dated photocopy of the original form which is to be kept by the service. These records must be retained for a period of at least four years from the ending of the authorisations to which they relate.

12.3 The Authorising Officer shall retain together the original Authorisation and Renewal forms until cancelled. On cancellation, the original Application, Renewal and Cancellation forms and any associated documents shall be retained in a closed file, in a secure place for at least four years after cancellation.

12.4 All information recovered through the use of a source which is relevant to the investigation shall be retained for at least five years after the cancellation of the authorisation or the completion of any Court proceedings in which said information was used or referred to. All other information shall be destroyed as soon as the operation is cancelled.

13. The Office of Surveillance Commissioners

13.1 The Office of Surveillance Commissioners (OSC) provides an independent overview of the use of the powers contained within the Regulation of Investigatory Powers (Scotland) Act 2000. This scrutiny includes inspection visits to local authorities by Inspectors appointed by the OSC.

14. Complaints

14.1 The Regulation of Investigatory Powers Act 2000 (the 'UK Act) establishes the independent Investigatory Powers Tribunal. This has full powers to investigate and decide any cases within its jurisdiction, including cases under RIP(S)A. Information on the Tribunal is available at http://www.ipt-uk.com/

14.2 The Council will ensure that copies of the Tribunal`s information sheet, its complaint form and its Human Rights Act claim form will be made available by accessing the Council`s internet site and if a request is made for one or more of these at a public Council office it should be downloaded from the internet and given to the requester. These documents can be downloaded from the complaints page .

14.3 To better inform potential complainers there is a requirement to make available for reference copies of the relevant Codes of Practice produced by the Scottish Ministers. These will be made available at public offices of Dumfries and

Galloway Council by downloading from the Scottish Government's website as well as being accessible through the Council`s internet web-site through the following hyperlink - http://www.scotland.gov.uk

15. Policy Review

This policy shall be reviewed on an annual basis and approved by Elected Members.

.

CHIS Policy and Procedures end.