THE MORAY COUNCIL: POLICY AND AUTHORISATION PROCEDURE ON COVERT SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCES

1.0 INTRODUCTION

1.1 In some circumstances, it may be necessary for council employees, in the course of their duties, to make observations of a person or person(s) 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 (in the ordinary sense of the word) and may give rise to legal challenge 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).

1.2 The Regulation of Investigatory Powers Act (2000) ("RIPA") and the Regulation of Investigatory Powers (Scotland) Act (2000 ("RIPSA")) together provide a legal framework both for authorising covert surveillance and covert human intelligence sources ("undercover" officers or informants) by public authorities and for an independent inspection regime to monitor these activities within the United Kingdom.

2.0 OBJECTIVE

2.1 The objective of this policy is to ensure that all covert surveillance and covert human intelligence sources (CHIS) used by council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the then Scottish Executive's Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources ('the Codes of Practice').

2.2 If the procedures outlined in this policy are not followed, any evidence obtained as a result of the surveillance may be open to challenge. This may result in the Procurator Fiscal deciding not to prosecute the case, or in the case later failing because the evidence is deemed to be inadmissible by the court. The Council may also be vulnerable to legal action by individuals who claim that their right to privacy has been infringed.

3.0 PUBLICITY

3.1 Copies of this Policy and the Codes of Practice shall be available for inspection by any person at the Council Headquarters, Council Offices, High Street, Elgin and at Access Points and Libraries throughout Moray and also on the Council's webpages.

4.0 COMPLAINTS TO THE INVESTIGATORY POWERS TRIBUNAL

4.1 Any person who is aggrieved by any conduct which falls within the scope of this procedure, and which has taken place in relation to that person or to any property of that person and has taken place in challengeable circumstances, is entitled to complain to the Tribunal at the following address:

Investigatory Powers Tribunal
PO Box 33220
LONDON
SW1H 9ZQ

5.0 SCOPE OF THE PROCEDURE

5.1 This procedure applies in all cases where directed surveillance or the use of a covert human intelligence source is being planned or carried out:-

(a) Directed surveillance is defined 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" [Scottish Executive Code of Practice on Covert Surveillance, para 1.7]

The procedure does not apply to observations that are not carried out covertly, or to unplanned observations made as an immediate response to events. As a result, it does not apply to the use of overt CCTV systems unless these systems are used as part of a pre-planned operation or investigation, in which event authorisation may be necessary. Equally, this procedure does not apply to ad-hoc covert observations that do not involve the systematic surveillance of specific person(s). In cases of doubt, the authorisation procedures described below should however be followed.

(b) A covert human intelligence source (CHIS) is defined as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that:-

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

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

6.0 PRINCIPLES OF SURVEILLANCE

6.1 In planning and carrying out covert surveillance or using or conducting a CHIS, Moray Council employees shall comply with the following principles.

6.2 Lawful purposes - covert surveillance or CHIS operations shall only be carried out where this is necessary to achieve one or more of the permitted purposes i.e. it must be:

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

(ii) in the interests of public safety;

(iii) for the purpose of protecting public health.

6.3 Employees carrying out surveillance shall not cause damage to any property or harass any person. Authorisation of use or conduct of a CHIS does not amount to a licence to commit a crime. Any source who acts beyond acceptable limits will not be protected from prosecution by the authorisation.

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

(ii) Effectiveness - planned covert surveillance/CHIS operations shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

(iii) Proportionality - the use and extent of covert surveillance/a CHIS shall not be excessive i.e. the methods of surveillance used must not be more intrusive than is warranted by the seriousness of the criminal or undesirable activity under investigation.

(iv) Intrusive surveillance- no activity shall be undertaken that comes within the definition of 'Intrusive Surveillance', i.e. if it involves surveillance of anything taking place on residential premises or in a private vehicle, whether from within or outside. Intrusive surveillance may only be authorised by the Chief Constable and so Local Authority officers should only very rarely be involved in this type of surveillance. "Residential premises" include any premises occupied or used, however temporarily, for residential purposes, but are not thought to include common areas such as common stairs and closes. Devices carried into a home or private vehicle by a CHIS do not also require authorisation as intrusive surveillance if the CHIS has been invited in. However, if the device is to be left behind when the CHIS leaves, this would require authorisation by the Chief Constable. The key issue is the presence of the CHIS whilst the surveillance is undertaken.

(v) Collateral intrusion - reasonable steps shall be taken to minimise the acquisition of information that is not directly necessary for the purposes of the investigation or operation being carried out. The applicant for an authorisation must detail in the application whether it is likely that there will be collateral intrusion and if so, confirm how this will be addressed in some detail. Information obtained due to collateral intrusion which was not anticipated at the time of the application must be disclosed to the Authorising Officer. The Authorising Officer will review the material at issue and order the destruction of anything irrelevant to the operation.

(vi) Authorisation - all directed surveillance and covert human intelligence sources shall be authorised in accordance with the procedures described below. Although it is possible to combine authorisation of two or more distinct types of surveillance under RIPSA, for example directed surveillance and the conduct of a source, in Moray this should be effected by submitting distinct applications and in turn, distinct authorisations will be granted if appropriate.

7.0 PARTICULAR ISSUES

7.1 Confidential Information

7.1.1 RIPSA does not provide any special protection for confidential information. It does however provide for 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.

7.1.2 “Confidential information” includes information subject to legal privilege, confidential personal information and confidential journalistic material.

7.1.3 Legal privilege attaches to most communications between a professional legal advisor and his client. Confidential personal information is information held in confidence relating to physical or mental health. Confidential journalistic material includes material created for journalism but supplied subject to an undertaking to hold it in confidence. Advice should be sought from Legal Services if any of these types of confidential information are likely to be involved in an operation.

7.2 Directed Surveillance

7.2.1 By definition, directed surveillance intrudes on people’s privacy as it will involve obtaining private information about someone.

7.2.2 “Private information” includes information about a person’s private or family life. The concept of private life is broadly interpreted. It includes not only personal information but also information about an individual’s relationships with others and can include how he runs his business and professional affairs. 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 is, the safest option is to seek authorisation.

7.2.3 Directed surveillance does not include entry on or interference with property or with wireless telegraphy. A separate regime for authorisation by the Chief Constable is set out in the Code of Practice.

7.3 CHIS

7.3.1 A CHIS may include individuals referred to as agents, informants and officers working undercover. The definition of CHIS requires that a relationship is established or maintained. This takes many test purchasing operations outwith this procedure as the carrying out of an everyday transaction does not of itself establish a relationship. If however the intention is for example for the CHIS to ascertain from the seller details of the supplier of counterfeit goods, when the seller took delivery of them etc that would entail the covert use of a relationship to obtain or provide access to information and would therefore require authorisation.

7.3.2 A number of different terms are used to describe those involved in CHIS operations:

7.3.3 **Handler** – means the person referred to in section 7(6) (a) of RIPSA 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

7.3.4 **Controller** – means the person (usually the line manager of the handler) within the local authority referred to in section 7(6) (b) of RIPSA responsible for general oversight of the source. The handler and controller may not be the same person.

7.3.5 The **conduct** of a source means the actions of that source falling within RIPSA or action incidental to it i.e. what the source does.

7.3.6 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

7.3.7 **Tasking** is the assignment given to the source. Either the handler or the controller may task a source. Tasking should be done only after authorisation for the use or conduct of the CHIS has been obtained. The only exception to this is where the source will not be establishing or maintaining a relationship for covert purposes, in which case authorisation may not be necessary.

7.3.8 From the above, it may be seen that both the conduct and the use of a CHIS require prior authorisation. This is effected through one application, but care must be taken to ensure that the authorisation complies with both procedures.

7.3.9 Although the safety and welfare of a source must always be taken into account in the risk assessment process, there are special procedures for the use or conduct of vulnerable individuals or juveniles (under 18 years of age) as a source. Reference should be made to the Code of Practice in this regard.

7.3.10 Insurance – all applicants for authorisation must ensure that they have all the necessary insurances for an operation e.g. vehicle insurance for use of the vehicle in surveillance.

8.0 SEEKING AUTHORISATION

8.1 When is authorisation required?

8.1.1 Authorisation is required for directed surveillance or the use or conduct of a CHIS, as defined in paragraph 5.1 above. 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.

8.1.2 Authorisation is required 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.

8.1.3 Advice as to whether an authorisation is required may be obtained via the Principal Solicitor, Litigation and Licensing.

8.2 Who may seek authorisation?

8.2.1 Any officer whose duties involve activity falling within the above descriptions may seek authorisation to do so and must seek authorisation prior to carrying out the surveillance described 5.1 above. Before submitting an application for the authorisation or renewal of authorisation for the use or conduct of a CHIS the officer seeking authorisation must first secure the approval of his or her line manager as the line manager will be required to act as controller relative to that source.

8.3 When is Covert Surveillance Appropriate?

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

9.0 THE AUTHORISATION PROCESS

9.1 Applications relative to covert surveillance and the use or conduct of a CHIS shall be authorised by the relevant authorising officer listed in Appendix 1 to this policy.

9.2 Forms for the application, review, renewal and cancellation of both directed surveillance and the use or conduct of a CHIS are detailed in section 12 below. In urgent cases, an oral application may be approved by the Authorising Officer, although he or she should make a written record of any urgent authorisations granted as soon as practicable thereafter. Urgent authorisations are only valid for a period of72 hours. If the operation requires to continue beyond the period authorised, in this case 72 hours, a renewal of the application must be authorised before that period has elapsed. Alternatively, the authorisation should be cancelled before the expiry of that period. A case is to be regarded as urgent so as to permit an authorisation to be given orally if the time taken to apply in writing would in the in the judgement of the authorising officer be likely to endanger life or to jeopardise the operation for which the authorisation is being given.

9.3 There are two situations where only the Chief Executive or (in his absence) his deputy may grant authorisations. The two exceptions are when knowledge of confidential information is likely to be acquired or when a vulnerable individual or a juvenile is to be used as a source.

9.4 All authorised officers listed in Appendix 1 must be of sufficient seniority as to fall within the scope of the Scottish Executive's guidance on authorising grades which is contained in the Regulation of Investigatory Powers (Prescription of Offices etc and Specification of Public Authorities) (Scotland) Order 2010; SSI 2010/350 and any amendments.

10.0 DUTIES OF OFFICERS

10.1 Duty of handler

10.1.1 In Moray the handler will also be responsible for maintaining the details required in terms of The Regulation of Investigatory Powers (Source Records) (Scotland) Regulations 2002; SSI No. 205 and any amendment thereof. Records to be maintained would include:

- The identity of the source
- The identity, where known, used by the source
- Any relevant investigating authority other than the authority maintaining the records
- The means by which the source is referred to within each relevant investigating authority
- Any other significant information connected with the security and welfare of the source
- Any confirmation made by a person 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 persons who, in relation to the source, are discharging or have discharged the functions mentioned in section 7(6)

(a) to (c) of RIPSA {i.e. the handler, the controller and the person responsible for maintaining a record of the use made of the source} or in any order made by the Scottish Ministers under section 7(2)(c)

- The periods during which those persons have discharged those responsibilities
- The tasks given to the source and the demands made of him or her in relation to their activities as a source
- All contacts or communications between the source and a person acting on behalf of any relevant investigating authority
- The information obtained by each relevant investigating authority by the conduct or use of the source
- Any dissemination by that authority of information obtained in that way and
- Any payment, benefit or reward and every offer of a payment, benefit or reward that is made by or on behalf of any relevant investigating authority in respect of the source's activities for the benefit of that or any other relevant investigating authority
- Any risk assessment made in relation to the source
- The circumstances in which tasks were given to the source
- The value of the source to the investigating authority

10.2 Duty of Authorising Officer

10.2.1 The Authorising Officer shall be responsible for:

- Deciding whether to authorise covert surveillance and ensuring that the authorisation is necessary for the period of the authorisation
- Diarising dates for reviews and renewals and ensuring that these are completed on schedule
- Refusing or cancelling authorisations where appropriate
- Reporting depersonalised annual RIPSA statistics to the Chief Legal Officer who will then arrange for all Council RIPSA Statistics to be reported to Full Council.
- Maintaining a full record of all documents and authorisations granted by them in a secure filing system.

10.2.2 In Moray the Authorising Officer will also be responsible for emailing to the Head of Legal and Democratic Services copies of relevant RIPSA documents to enable the Head of Legal and Democratic Services to maintain an electronic Central Register of Authorisations. These documents shall include:

- A copy of the application and authorisation together with any supporting documentation (including risk assessments) and notification of the approval given by the Authorising Officer;
- A copy of any application for renewal of an authorisation, together with the supporting documentation submitted when the renewal was requested
- A record of the reviews scheduled by the Authorising Officer together with the results of any reviews of the authorisation including any cancellations and the reasons for these.
- The reasons, if any, for not renewing an authorisation,
- The reasons for any refusals of authorisation

- The date and time when any instruction was given by the Authorising Officer to cease using a source
- A Matrix showing abbreviated details of all authorisations including the name, rank/grade of the Authorising Officer, the unique reference number (URN) of the investigation or operation, the title of the investigation or operation

11.0 ROLE OF SENIOR RESPONSIBLE OFFICER

11.1 The new codes of practice which came into on 5th February 2015, provided for the role of Senior Responsible Officer (SRO). The duties associated with this role include:-

- The integrity of the process in place within the public authority for the management of CHIS and DS authorisations;
- Compliance with RIP(S)A and the Codes of Practice;
- Oversight of the reporting of errors to the relevant oversight Commissioner and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- Engagement with the OSC inspectors when they conduct their inspections, where applicable; and
- Where necessary, oversight of the implementation of post-inspection action plans approved by the relevant oversight Commissioner.
- Report to the CMT on a six monthly basis
- Jointly report to P&R at the end of each financial year

12.0 ROLE OF MORAY RIPSA FORUM AND DUTIES OF THE CHAIR

12.1 Moray RIPSA Forum is a high level working group comprising officers from each service working with RIPSA. The Forum will be chaired by the Senior Responsible Officer.

12.2 The Forum will meet bi-annually to perform the following functions:

- To ensure that there is a high standard of training across the Council for relevant officers including cross-service training
- To keep this policy and procedure under review, including advising the SRO of any amendments necessary to the approved forms detailed in section 12
- To be consulted on reports of the Surveillance Commissioner, Internal Audit or any other reports concerning RIPSA

13.0 DOCUMENTS

13.1 This procedure requires the use of forms, copies of which are available on the RIPSA pages on Moray Council sharepoint. No other style of form may be accepted by the Authorising Officer, forms are approved and agreed by the Senior Responsible Officer.

14.0 REVIEW, RENEWAL AND CANCELLATION OF AUTHORISATION

14.1 Oral authorisations expire after 72 hours, directed surveillance authorisations after 3 months and CHIS authorisations after 12 months (except in the case of juvenile sources when the authorisation endures for only one month) all beginning at the date and time on which the authorisation took effect. Reliance should never be placed on the authorisation simply expiring however. To this end, the Authorising Officer shall review all authorisations at intervals of not more than one month, the review period being determined at the point of authorisation or renewal. The purpose of the review is to monitor the effectiveness of the surveillance and its continued necessity and proportionality.

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

14.3 At review or renewal the whole circumstances of the case must be fully considered in terms of RIPSA, this procedure and the relevant Code of Practice. The Risk Assessment form must also be reviewed.

14.4 The Authorising Officer shall cancel any authorisation as soon as he/she is satisfied that it no longer meets the criterion for authorisation. The Authorising Officer will then check the arrangements in place to terminate the surveillance and the Handler will then advise the source, if any, involved in the operation.

15.0 RISK ASSESSMENT

15.1 Although risk assessment is only a requirement in CHIS operations, it is good practice to conduct a risk assessment before embarking on any covert surveillance. This assessment should detail any possible risks to staff or other persons involved in or affected by an operation and should be completed on the Moray Council form approved for this purpose.

15.2 Before authorising any form of covert surveillance, the Authorising Officer should consider whether the proposed action would place any employee or other person at risk. If so, the Authorising Officer shall have regard to other council procedures already in place, and should also consider the risk assessment of the proposed course of action submitted with the application before authorisation is granted. The ongoing security and welfare of any source, after cancellation or expiry of the authorisation should also be considered.

16.0 MONITORING AND REVIEW

16.1 It shall be the duty of the Head of Legal and Democratic Services to monitor and review the authorisations granted by the Authorising Officer in terms of paragraph 10.2.2 to ensure that time periods have been observed, renewals and cancellations pursued where appropriate and that sufficient details are contained in applications and authorisations. The Head of Legal and Democratic Services shall twice yearly submit a report to the Senior Responsible Officer detailing his/her findings. The Head of Legal and Democratic services shall also prepare an annual report, jointly with the SRO, to P&R at the end of each financial year.

17.0 SECURITY AND RETENTION OF DOCUMENTS

17.1 Documents created under this procedure are highly confidential and must 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 Codes of Practice. It should be noted that refusals as well as approved applications must be retained. The Code of Practice recommends retention of RIPSA records for a period of 4 years from the ending of the authorisation.

17.2 Documents will be inspected periodically by the Office of the Surveillance Commissioner which has statutory powers of inspection. No records should be destroyed until after they have been inspected by the Surveillance Commissioner.

17.3 Each Department shall maintain a register of current and past authorisations, renewals, refusals and cancellations. Copies of all such completed forms will be passed to the Chief Legal Officer (as Monitoring Officer) electronically who shall maintain a central register of all forms submitted by officers for authorisation under RIPSA all in accordance with paragraph 10.22 & 15.1

Appendix 1

List of Authorising Officer Posts

Environmental Services Department

- Corporate Director
- Head of Development Services
- Trading Standards Manager
- Environmental Health Manager

Chief Executive

- Must authorise where operation likely to obtain confidential information.
- Must authorise when a vulnerable individual or juvenile (under 18 years of age) is to be used as a source.