MIDLOTHIAN COUNCIL

COVERT HUMAN INTELLIGENCE SOURCES POLICY AND GUIDANCE

Document Control Information

Revision	Date	Revision Description
Version 1.0	19/5/16	
Version 2.0	26/03/2019	3 yearly review
Version 3.0	23/06/2020	Updated to reflect change in Council Structure
Version 4.0	18/01/2023	Updated to reflect comments from ICPO and appoint new Authorising Officer

	INDEX	Page
1	Introduction	3
2	Scope of Policy	3
3	Relationship with the Policy on Surveillance	4
4	Principles of Use of Covert Human Intelligence Source	5
5	The Authorisation Process	6
6	Confidential Material	7
7	Vulnerable and Juvenile Sources	7
8	Management of Sources	8
9	Security and Retention of Documents	9
10	Oversight	10
11	Complaints	10
12	Review	10

POLICY AND GUIDELINES ON COVERT HUMAN INTELLIGENCE SOURCES

See also separate Policy and Guidelines on Covert Surveillance

1. INTRODUCTION

Under section 1(7) of the Regulation of Investigatory Powers (Scotland) Act 2000 ("RIPSA"), a person is a Covert Human Intelligence Source (commonly referred to as a "CHIS") if he or she:

(a) establishes or maintains a personal or other relationship with a person for the covert purpose of facilitating the doing of anything falling within (b) or (c) below and either:
(b) covertly uses such a relationship to obtain information or to provide access to any information to another person; or
(c) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

It is important to note that the Council is obliged to follow the Code of Practice issued by Scottish Ministers in 2017 in regard to every authorisation of the use of a Covert Human Intelligence Source under RIPSA. Failure to do so may be founded upon in any criminal or civil proceedings.

This policy should also be read in conjunction with the Procedures and Guidance issued by the Office of Surveillance Commissioners (OSC).

Copies of the Code of Practice and the Procedures and Guidance are available via the Midlothian Council Intranet.

The Code of Practice and the Procedures and Guidance can also be accessed through the links below and all staff working with Covert Human Intelligence Sources are expected to be familiar with these documents:

http://intranet/services/webinfo/WebInfoPDF.asp?BlobID=24378

https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/OSC-PROCEDURES-AND-GUIDANCE.pdf

2. SCOPE OF THE POLICY

This procedure applies in all cases where a "Covert Human Intelligence Source" is to be used. Covert Human Intelligence Source (hereinafter referred to as a source) is defined by Section 1(7) of the RIPSA. A person will be acting as a source if they covertly (i.e. without disclosing their true purpose) establish or maintain a personal or other relationship with another person in order to obtain information from that person or to disclose information obtained from that person or to provide access to information to another person. The definition of a source is not restricted to obtaining private information.

A local authority may therefore use a source in two main ways. Employees of the Midlothian Council may themselves act as a source by failing to disclose their true identity in order to obtain information. Alternatively an employee of the Midlothian Council may cultivate a member of the public or employee of a business under investigation to provide them with information on a regular basis. This person will also be acting as a source. In both cases the person or persons being investigated are unaware that this is taking place.

The procedure does not apply in circumstances where members of the public volunteer information on an initial basis as part of their normal civic duties or contact numbers specifically set up to receive anonymous information such as crime-stoppers. However, someone might become a source as a result of a relationship with the Midlothian Council that began in this way and authorisation must then be sought.

Further examples of when this procedure will apply and an individual considered to be a Source are contained in Chapter 2 of the Code of Practice.

It is also noted that an explicit statutory power may exist under other legislation authorising employees of the Council to carry out certain activities such as test purchasing. Where statutory authority exists under other legislation it will not normally be necessary to seek authorisation under this procedure. However, where the activity requires the officer to establish a personal relationship with any person or where the activity concerned takes place on premises which are also residential or in a situation where a high degree of privacy would be expected then authorisation under this procedure must also be sought.

Staff must be aware of the possibility of status drift when an individual develops into a source eg through the repeated provision of information about an individual, a relationship develops in test purchasing or a staff member responds to, posts on or otherwise interacts on an individual's Social Networking Site. Staff should monitor for status drift and take appropriate action including seeking authorisation if they think it has occurred.

3. RELATIONSHIP WITH THE POLICY ON COVERT SURVEILLANCE

Where it is envisaged that the use of a source will also be accompanied by directed surveillance then authorisation must also be sought under the Council's policy on covert surveillance.

Where a source wearing or carrying a surveillance device is invited into residential premises or a private vehicle separate authorisation is not required under the surveillance procedure as long as the Council's procedure on Covert Human Intelligence Sources has been followed and authorisation given.

Where the source themselves is subject to surveillance to identify whether they would be an appropriate person to act as a source this surveillance must be authorised in accordance with the surveillance procedure

4. PRINCIPLES OF USE OF COVERT HUMAN INTELLIGENCE SOURCE

Where planning and making use of a source Midlothian Council employees shall comply with the following principles:

Lawful purposes - A source shall only be used where necessary to achieve one or more of the permitted purposes (as defined in the Act) namely:

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

(b) in the interests of public safety; or

(c) for the purpose of protecting public health.

Necessity - A source should only be utilised where there is no reasonable and effective alternative way of achieving the desired objective(s).

Proportionality – using a source shall be proportionate and shall not be excessive i.e. the use of a source shall be in proportion to the significance of the matter being investigated and the information being sought could not reasonably be obtained by other means. Particular care should be taken if the source is likely to obtain information in a situation where the person under investigation would expect a high degree of privacy

Collateral intrusion – Consideration must be given to the extent to which the use and conduct of the source will interfere with the privacy of persons other than the subject of the investigation and to minimise the impact on them. Reasonable steps shall also be taken to minimise the acquisition of information that is not directly necessary for the purposes of the investigation or operation being carried out. If the investigation unexpectedly interferes with the privacy of individuals not covered by the authorisation consideration must be given to whether a new authorisation is required.

Effectiveness - tasking and managing the source shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

Authorisation – the use of all sources shall be authorised in accordance with the procedures described below.

The same principles and procedures on authorisations apply as in the Surveillance Policy. Application forms for a) CHIS authorisation, b) review, c) renewal and d) cancellation are appended to this Policy. In the case of CHIS, by law the authorisation lasts for twelve months (instead of three).

Just as with cases likely to involve the acquisition of Confidential Information, only the Chief Executive may grant authorisations when a “vulnerable individual” is authorised to act as a CHIS, and then only in exceptional cases. A “vulnerable individual” is a person who is or may be in need of community care services by reason of mental or other disability, age or illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation.

This restricted authorisation procedure also applies to the use or conduct of juvenile sources, that is any CHIS under the age of 18 years. On no occasion should the use or conduct of a source under 16 years of age be authorised to give information against his parents or any person who has parental responsibility over him. In other cases, authorisations should only be granted if the special provisions of The Regulation of Investigatory Powers (Juveniles) (Scotland) Order 2002 apply and the duration of such authorisations will be only one month.

5. THE AUTHORISATION PROCESS

As detailed in the Council’s policy on Covert Surveillance, Authorisations may only be granted/reviewed/renewed and cancelled by:

- The Chief Executive;
- Executive Director, Place;
- Executive Director, Children, Young People and Partnerships;
- The Chief Officer, Place; or
- The Legal and Governance Manager.

In accordance with the Code of Practice authorisations will last 12 months. The person responsible for authorising the surveillance must ensure that the authorisation is reviewed at least monthly and those authorisations that are no longer needed or appropriate are cancelled.

All reviews must be documented and will need to be carried out more frequently where there exists a risk of acquiring confidential material or where the source is a juvenile or deemed vulnerable.

The Executive Director, Place has been appointed as the Council’s Senior Responsible Officer. As such, it is good practice that the Senior Responsible Officer does not grant authorisations but he is competent to do so if other Authorising Officers are not available.

Each Division will keep a record of any applications that are refused by the authorising officer. Any refusal shall also be recorded in the Central Register.

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.

The Code of Practice should be referred to for the detailed rules on tasking sources, management responsibility and special provisions on recording of

telephone conversations and the use of technical equipment. In particular, it should be noted that a risk assessment should be carried out which takes full account of the security and welfare of the source.

6. CONFIDENTIAL MATERIAL

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

Confidential material consists of:

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

Such applications shall only be granted in exceptional and compelling circumstances where the authorising officer is fully satisfied that this conduct is both necessary and proportionate in these circumstances. If granted such authorisation will last 1 month. Where any confidential material is obtained then the matter must be reported to the Investigatory Powers Commissioner's office during their next inspection and any material obtained made available to them if requested. Reviews may need to be more regularly carried out than monthly where the source provides access to confidential material or where collateral intrusion exists.

7. VULNERABLE AND JUVENILE SOURCES

Particular care must be taken where authorising the use or conduct of vulnerable or juvenile individuals to act as sources. The code of practice defines a vulnerable individual as "a person who is or may be in need of community care services by reason of mental or other disability, age, illness and who is or may be unable to take care of himself, or unable to protect himself against significant harm or exploitation."

Vulnerable individuals should only be in authorised to act as a source in the most exceptional circumstances. Authorisation may only be granted on the approval of the Chief Executive. Prior to deciding whether or not to grant such approval the Chief Executive shall seek the advice of the Chief Social Work Officer on the appropriateness of using the individual in question as a CHIS. If granted such authorisation will last 1 month.

A juvenile is any person under the age of eighteen. On no occasion should the use of a source under sixteen years of age be authorised to give information against his or her parents or any person who has parental responsibilities for him or her.

In other situations authorisation for juveniles to act as a source may only be granted on the approval of a Chief Executive and only with the prior advice of the Chief Social Work Officer as described above.

When considering the appropriateness of any individual to become a source, extreme care must be taken to ensure that the identity of the individual is not disclosed.

The following conditions must also be met:

- a risk assessment must be undertaken to identify any physical and psychological aspects of their deployment. This risk assessment must be carried out in conjunction with a registered social worker from a relevant discipline i.e. children and families, criminal justice or community care;

- the authorising officer must be satisfied that any risks have been properly explained; and

- the authorising officer must give particular consideration to the fact that the juvenile is being asked to obtain information from a relative, guardian or other person who has assumed responsibility for their welfare

An appropriate adult e.g. social worker or teacher must also be present at any meetings between the authority and a source under 16 years of age and the maximum authorisation period that can be granted for a juvenile or vulnerable source is one month.

8. MANAGEMENT OF SOURCES

Before authorisation can be given, the authorising officer must be satisfied that suitable arrangements are in place to ensure satisfactory day to day management of the activities of a source and for overseeing these arrangements.

An individual officer must be appointed to be responsible for the day to day contact between the source and the authority including:

- Dealing with the source on behalf of the 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.

In addition the authorising officer must satisfy themselves that an officer has been designated responsibility for the general oversight of the use made of the source.

The authorising officer must also ensure that a risk assessment is carried out to determine the risk to the source of any tasking and the likely consequences

if the role of the source becomes known. It will be the responsibility of the officer in day to day control of the source to highlight any concerns regarding the personal circumstances of the source which may affect the validity of the risk assessment, the conduct of the source or the safety or welfare of the source.

Records must also be maintained, in accordance with the relevant statutory instruments, detailing the use made of the source.

It will be the responsibility of the person in day to day control of the activities of the source to maintain the relevant records.

The following matters must be included in the records relating to each source:

(i) identity of the source and the means by which the source is referred to;
(ii) the date when and the circumstances within the source was recruited;
(iii) the name of the person with day to day responsibility for the source and the name of the person responsible for overall oversight;
(iv) any significant information connected with the security and welfare of the source;
(v) confirmation by the authorising officer that the security and welfare of the source have been considered and any risks have been fully explained and understood by the source;
(vi) all contacts between the source and the local authority;
(vii) any tasks given to the source;
(viii) any information obtained from the source and how that information was disseminated;
(ix) any payment, benefit or award or offer of any payment, benefit or award or offer given to a source who is not an employee of the local authority; and
(x) any relevant investigating authority other than the authority maintaining the records.

9. SECURITY AND RETENTION OF DOCUMENTS

Documents created under this procedure are highly confidential and shall be treated as such. Divisions shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 2018 and the Code of Practice.

In addition each Division shall also ensure arrangements are in place for the handling, storage and destruction of material obtained through a source in accordance with the requirements of the Data Protection Act 2018 and the Code of Practice.

All material obtained as result of the activities of a source must be retained if it is believed that it is relevant to that investigation or to pending or future criminal or civil proceedings. It must be retained until its review suggests that the risk of legal proceedings no longer exists or having taken place has now been resolved.

Extreme care must be taken to ensure that the identity of the individual is not disclosed.

10. OVERSIGHT

Internal oversight is provided by the Council's Senior Responsible Officer. The Senior Responsible Officer is a member of the Corporate Management Team and is responsible for the integrity of the internal processes within Midlothian Council for the management of Covert Human Intelligence Sources and for Council compliance with RIPSA and the Code of Conduct.

The Investigatory Powers Commissioner's Office (IPCO) provides independent oversight of the use of the powers contained within the Regulation of Investigatory Powers Act 2000 and Regulation of Investigatory Powers (Scotland) Act 2000. This oversight includes inspection visits by Inspectors appointed by the IPCO.

11. COMPLAINTS

The Regulation of Investigatory Powers Act 2000 (the 'UK Act') establishes an independent tribunal. This tribunal has full powers to investigate any complaints and decide any cases within the United Kingdom including complaints about activities carried out under the provisions of The Regulation of Investigatory Powers (Scotland) Act 2000. Details of the relevant complaint procedure can be obtained from the Investigatory Powers Tribunal, PO Box 33220, London, SW1H 9ZQ.

12. REVIEW

This policy will be reviewed every three years from the date of approval.

APPENDICES

Covert Human Intelligence Source Application Form	-	Appendix 1
Covert Human Intelligence Source Review Form	-	Appendix 2
Covert Human Intelligence Source Renewal Form	-	Appendix 3
Covert Human Intelligence Source Cancellation Form	-	Appendix 4


CHIS Application - FINAL.doc


CHIS Review - FINAL.doc


CHIS Renewal - FINAL.doc


CHIS Cancellation - FINAL.doc

These forms can be accessed on the Intranet via Council/Legal/Surveillance Guidance.