Corporate Policy and Strategy Committee

10am, Thursday, 25 February 2014

Update of Council Surveillance Policies

Item number	7.7
Report number	
Wards:	All

Links

Coalition pledges:	P34
Council outcomes:	
Single Outcome Agreement:	SO4

Mark Turley

Director of Services for Communities

Contact: Susan Mooney, Head of Service

Email: susan.mooney@edinburgh.gov.uk | Tel: 0131 529 7587

Andrew Mitchell, Community Safety Manager

Email: andrew.mitchell@edinburgh.gov.uk | Tel: 0131 469 5822

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Executive summary

Update of Council Surveillance Policies

Summary

The Council is authorised to make use of the provisions of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) and, in relation to communications data, the Regulation of Investigatory Powers Act 2000 (RIPA).

This report updates the Committee on the successful outcome of an inspection by the Office of Surveillance Commissioners (OSC) in June 2013, and recommends for approval some minor amendments to existing Council policies relating to the use of surveillance.

It also submits a new policy on the Acquisition of Communications Data for approval.

Recommendations

1 Committee is asked to:

a) note the successful outcome of the OSC inspection in June 2013.

b) approve the revised surveillance policies attached at Appendix 1 and Appendix 2. These policies relate to the provisions of the Regulation of Investigatory Powers (Scotland) Act 2000.

c) approve the policy on the Acquisition of Communications Data attached at Appendix 3. This policy relates to the provisions of the Regulation of Investigatory Powers Act 2000.

Measures of success

The use of RIPSA and RIPA remains a last resort.

Where the powers are utilised they are subject to strict control and the Council complies with all relevant duties.

The Council continues to perform well when subject to statutory inspection by the relevant inspection bodies.

The policy contributes to effective action to maintain community safety.

Financial impact

There is no financial impact from amending existing policies.

Equalities impact

The attached policies have a high degree of relevance to the Council's duties under the Human Rights Act 1999. There are no adverse impacts on any group or individual with a protected characteristic.

Sustainability impact

This report is not relevant to sustainability issues.

Consultation and engagement

The revised policies have been reviewed by the Council's RIPSA Authorising Officer Group which includes representation from Legal, Risk and Compliance.

Background reading / external references

None.

Report

Update of Council Surveillance Policies

1. Background

1.1 The Council is authorised to use certain surveillance powers under the Regulation of Investigatory Powers (Scotland) Act 2000. The Council is additionally authorised to use certain surveillance powers under the Regulation of Investigatory Powers Act 2000, specifically relating to telephone or email subscriber details only.

1.2 The Council is subject to external oversight in relation to how it uses both Acts. On 10 June 2013 the Council was subject to an inspection by the Office of Surveillance Commissioners (OSC). The purpose of the inspection was to assess the Council's compliance with the legal requirements of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA).

1.3 The Council's RIPSA policies have been in place for several years. Following the inspection of 10 June 2013, minor amendments to the policies were required in order to discharge the recommendations made by OSC.

1.4 The Regulation of Investigatory Powers Act 2000 (RIPA) is UK-wide legislation, allowing in particular the acquisition of communications data in certain circumstances. The legislation was amended by the Protection of Freedoms Act 2012, and as a result it is prudent that a policy be introduced to strengthen the governance of this issue.

2. Main report

2.1 **Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA)**

As a relevant public body, the Council is authorised to use surveillance for the following purposes:

- preventing or detecting crime or disorder;
- protecting public health;
- in the interests of public safety

These powers are typically used to investigate complaints about antisocial behaviour, breaches of trading standards or environmental health legislation, or benefit fraud. In the last three financial years the powers have been used on average 26 times per year. The Council is not authorised to use what is referred to as 'Intrusive Surveillance,' which involves surveillance targeting domestic premises, this power is reserved to the Police.

2.2 The Council is subject to rigorous inspection by the Office of Surveillance Commissioners (OSC). The Council has been inspected five times since the Act came in to force. The inspection audits the use of the powers by Council officers, and reviews the governance arrangements in place to ensure that the Act is fully complied with.

2.3 On 10 June 2013 OSC carried out its latest inspection. The inspection report was overwhelmingly positive and concluded that:

- "Overall the City of Edinburgh Council is a well performing council".
- Officers responsible for the operation of RIPSA, "impressed with both their enthusiasm and knowledge".
- "The management structure is of the highest standard and involves processes which are rarely seen in other local authorities".

2.4 The report noted that several improvements had been made since the previous inspection in June 2010. There were some issues for the Council to address in order to ensure that Authorising Officers better document the process undertaken when dealing with an application.

2.5 The OSC inspector pointed out some minor anomalies in the existing policies. The opportunity has been taken to address these and to update the policies. A revised policy on Covert Surveillance is attached at Appendix 1 and a revised policy on the use of Covert Human Intelligence Sources (CHIS) is attached at Appendix 2.

2.6 The following changes have been made to the policies:

- Updated to reflect changes in the Council's organisational structure.
- In relation to certain types of surveillance (where there is a risk of obtaining 'Confidential Information' and use of certain (CHIS)) the time period of authorisation has been amended to reflect statutory guidance.

Regulation of Investigatory Powers Act 2000 (RIPA)

2.7 In certain limited circumstances RIPA allows public authorities (including the Council) to ask a communications service provider for information about subscribers to its service. Checks are completed without the subscriber being made aware of the check; in other words the check is covert.

2.8 This information can be requested if the purpose is the prevention or detection of crime, or the prevention of disorder. These are narrower grounds than those specified by RIPSA. A separate statutory inspection framework exists for RIPA, to date the Council has not been subject to inspection. Use of RIPA is much more limited than use of RIPSA, and RIPA applications average 10 per year.

2.9 Examples of Council use of RIPA can include, for example, investigation of sales of counterfeit or unsafe goods via Facebook or other websites, or tracing itinerant traders or unnamed sellers who use mail boxes. The Council is <u>not authorised</u> to seek or obtain the content of any communication e.g. the content

of any email or text message and would in no circumstance seek such information.

2.10 The legislative framework covering RIPA has recently changed as a result of the Protection of Freedoms Act 2012. Applicants are now required to obtain judicial approval before the acquisition of communications data will be authorised. Prior to this change there was no judicial oversight. In Scotland public authorities must make such an application to a Sheriff.

2.11 The Council's first successful application since the regime was changed was recently made by the Trading Standards Service in the autumn of 2013. This case involved tracing an itinerant trader who was alleged to have coerced a consumer to accept substantial works to their home and failed to provide the consumer with cancellation rights.

2.12 To ensure a clear and consistent approach across RIPA and RIPSA Committee is asked to approve the draft Policy on Acquiring Communications Data which is attached at Appendix 3.

3. Recommendations

3.1 Committee is asked to:

a) note the successful outcome of the OSC inspection in June 2013.

b) approve the revised surveillance policies attached at Appendix 1 and Appendix 2. These policies relate to the provisions of the Regulation of Investigatory Powers (Scotland) Act 2000.

c) approve the policy on the Acquisition of Communications Data attached at Appendix 3. This policy relates to the provisions of the Regulation of Investigatory Powers Act 2000.

Mark Turley

Director of Services for Communities

Links

Coalition pledges	Work with police on an anti-social behaviour unit to target persistent offenders
Council outcomes	
Single Outcome Agreement	Edinburgh's communities are safer and have improved physical and social fabric
Appendices	Appendix 1: RIPSA policy (directed surveillance) Appendix 2: RIPSA procedure (CHIS) Appendix 3: Draft RIPA policy

Policy on Directed Surveillance

Policy on Directed Surveillance

Policy Statement

In some circumstances it may be necessary for the City of Edinburgh Council employees, in the course of their duties, to make observations of a person or persons in a covert manner, i.e. without that person's knowledge. By their 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 of the European Convention on Human Rights and the Human Rights Act 1998 ('the right to respect for private and family life').

The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) ('the Act') provides for the first time a legal framework for covert surveillance by public authorities (including local authorities) and an independent inspection regime to monitor these activities.

Whilst the Acts do not impose a requirement for local authorities to seek or obtain an authorisation the City of Edinburgh Council employees however will, wherever possible, adhere to the authorisation procedure before conducting any covert surveillance.

Authorising Officers within the meaning of this procedure shall avoid authorising their own activities wherever possible and only do so in exceptional circumstances.

No activity shall be undertaken by employees of the City of Edinburgh Council that comes within the definition of 'Intrusive Surveillance'. Intrusive Surveillance is covert surveillance of anything taking place on residential premises or in a private vehicle that either involves the presence of an individual or surveillance device on the premises or in the vehicle or is carried out by means of a surveillance device located elsewhere 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 residential premises.

An annual report will be submitted to members summarising the use of surveillance under this policy.

Scope

This procedure applies in all cases where 'directed surveillance' is being planned or carried out. Directed surveillance is defined by RIPSA as covert surveillance undertaken "for the purposes of a specific investigation or a specific operation" and "in such a manner as is likely to result in the obtaining of private information about a person" whether or not that person is the target of the operation and other than by way of an immediate response to events or circumstances (Section 1(2) RIPSA).

The procedure does not apply to:

- observations that are carried out overtly, or
- unplanned observations made as an immediate response to events where it was not reasonably practicable to obtain authorisation
- non-planned, ad hoc covert observations that do not involve the systematic surveillance for a specific investigation or operation
- **any disciplinary investigation or any activity involving the surveillance of employees of the Council, unless such surveillance directly relates to a regulatory function of the Council.**

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

The objective of this procedure is to ensure that all covert surveillance by the City of Edinburgh Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the relevant legislation, the Scottish Government's Code of Practice on Covert Surveillance ('the Code of Practice') and any guidance which the Office of Surveillance Commissioners may issue from time to time. Copies of the Code of Practice must be available for public reference at all offices of the local authority and be made available to all staff involved in surveillance operations.

This procedure does not apply to Closed Circuit Television (CCTV) installations where there is a reasonable expectation that members of the public are aware that an installation is in place (overt surveillance), normally this would be demonstrated by signs alerting the public to the CCTV cameras.

However where an employee, other than in immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation to be sought, directs surveillance via CCTV equipment then authorisation should be sought **no later than the next working day.**

If an operator of any Council CCTV system is approached by any other employee or other agency requesting that the operator undertake Directed Surveillance using CCTV, the operator is required to obtain a written copy of a RIPSA authorisation prior to such use. This authorisation must detail the use of a specific camera system for the purpose of directed surveillance. The authorisation must be signed by either one of the

Council's Authorising Officers or in the case of the Police, 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 can be accepted. A copy should be kept and the original forwarded to Legal Services for noting in the central register.

If the operator is unsure about an aspect of the procedure they should refer to the Council's code of practice for CCTV operation or seek advice from their line manager.

Definitions

'Covert surveillance' means surveillance that is carried out in a manner calculated to ensure that the persons subject to the surveillance are unaware that it is or may be taking place.

Intrusive Surveillance is covert surveillance of anything taking place on residential premises or in a private vehicle that either involves the presence of an individual or surveillance device on the premises or in the vehicle or is carried out by means of a surveillance device located elsewhere 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 residential premises.

Policy content

Principles of Surveillance

In planning and carrying out covert surveillance, the City of Edinburgh Council employees shall comply with the following principles:

Lawful purposes – covert surveillance shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in the Act) namely:

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

(ii) in the interests of public safety;

(iii) for the purpose of protecting public health;

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

Proportionality – the use and extent of covert surveillance shall be proportionate and not excessive i.e. its use shall be in proportion to the significance of the matter being investigated and the information being sought cannot reasonably be obtained by other less intrusive means.

Collateral intrusion – Consideration must be given to the extent to which the surveillance will interfere with the privacy of persons other than the subject of the surveillance and to minimise the impact of the surveillance 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.

Effectiveness – planned covert surveillance shall be undertaken only by suitably trained or experienced employees, or under their direct supervision.

Authorisation – all directed surveillance shall be authorised in accordance with the procedures described below.

The Authorisation Process

Subject to the exception detailed below, applications for directed surveillance will be authorised at the level of Investigations Manager or Head of Service as prescribed by the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Order 2010. The current list of Council Officers designated to authorise directed surveillance is agreed by the Chief Executive and available on the Orb. Authorising Officers should be suitably trained in terms of the requirements of the Regulation of Investigatory Powers (Scotland) Act 2000. The Head of Service, Community Safety shall circulate to all relevant service areas any changes to the list of Council Officers designated to authorise directed surveillance.

Applicants should apply within their own line management structure unless other arrangements have been agreed or it is unreasonable or impractical in the circumstances. Authorising Officers shall not be responsible for authorising their own activities.

Authorisations must be given in writing. In urgent cases only, an Authorising Officer may approve oral applications. An application in writing indicating the reasons why an oral authorisation was sought must then be made as soon as reasonably practicable. In any case an oral authorisation will expire after 72 hours. If surveillance is to continue after the 72 hours a further application in writing must be made.

In accordance with the Code of Practice authorisations will last three 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 cancelled. All reviews must be documented **using Form CEC/RIPSA/DS4 Review of Directed Surveillance and shall also be recorded in the central register.** Reviews will need to be carried out more frequently where the surveillance provides access to confidential information or involves collateral intrusion.

Each Service area 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.

Services wishing to adopt a more devolved authorisation process may do so only on the explicit approval of a written policy by the Council; all authorisations must remain within the scope of the Scottish Government's guidance on authorisation.

Confidential Material

Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of the Chief Executive acting as Authorising Officer. In their absence a Director may deputise as Authorising Officer.

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 surveillance is both necessary and proportionate in these circumstances. In accordance with the Code of Practice such authorisations will last three months. Where any confidential material is obtained then the matter must be reported to Office of Surveillance Commissioners during their next inspection and any material obtained made available to them if requested.

Documents

This procedure uses the following documents **which shall be used by all Service areas:**

Application for Authority for Directed Surveillance (Form CEC/RIPSA/DS1)
The applicant should complete this in all cases, including where oral authorisation was first sought. It is effective from the time that approval is given.

Application for Renewal of Directed Surveillance Authority (Form CEC RIPSA/DS2)
This should be completed where a renewal for authorisation is applied for.

Cancellation of Directed Surveillance (Form CEC/RIPSA/DS3)
The applicant and the Authorising Officer should complete this when the authorisation ceases to be either necessary or appropriate.

Review of Directed Surveillance (Form CEC/RIPSA/DS4)
The Authorising Officer should complete this when carrying out reviews of the authorisation.

Additional Sheet for Authorising Officers to complete if required (Form EC/RIPSA/AS1)

Security and Retention of Documents and Materials

Documents created under this procedure are highly confidential and shall be treated as such. Service areas 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.

In addition each Service area shall also ensure arrangements are in place for the handling, storage and destruction of material obtained through directed surveillance in accordance with the requirements of the Data Protection Act 1998 and the Code of Practice.

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

Central Register

The Head of Legal, Risk and Compliance shall maintain a register of current and past authorisations and of any applications for authorisations that have been refused. Each Service area will provide Legal Services with all original documentation relating to authorisations under the Regulation of Investigatory Powers (Scotland) Act 2000 including cancellations, renewals and reviews within three working days of the action being taken. Authorising Officers shall ensure that sufficient information is provided to keep this up to date.

Each authorisation will be given a unique reference number prefaced by a Service area number in brackets. The central register will contain the following information:

- Type of authorisation e.g. Directed Surveillance or Covert Human Intelligence Source
- Start date of the authorised activity
- Whether the application was authorised or refused
- Date of authorisation / refusal
- Name and Title of the Authorising Officer
- Title of the investigation or operation, if known including a brief description and names of subjects
- Whether the urgency provisions were used and if so why
- Confirmation that the Authorising Officer did not authorise their own activities
- Date of review

- Date of renewal and who authorised the renewal
- Date of cancellation
- Whether the investigation is likely to result in obtaining confidential information as defined in the Code of Practice

The Head of Legal, Risk and Compliance will provide regular monitoring information to Service areas.

The central register records must be retained for a period of at least three years from the ending of the authorisation or for a further suitable period if relevant to pending court proceedings

Oversight

The Office of Surveillance Commissioners (OSC) 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 OSC.

Equalities and Rights Impact Assessment

A full Equalities and Rights Impact Assessment has been carried out in respect of this policy, and is available on request. There was no resulting indication of unlawful practice or violation of rights.

Strategic Environmental Assessment

This policy has no relevance to environmental issues and therefore an assessment is not practical.

Implementation

This policy will be implemented by each service area. Appropriate briefings shall be carried out. Authorising Officers shall be trained appropriately.

The success of the policy will be measured against a positive outcome in any statutory inspection of the Council.

Authorisation process

Subject to the exception detailed below applications for directed surveillance will be authorised at the level of Investigations Manager or Head of Service as prescribed by the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Order 2010. The current list of Council Officers designated to authorise directed surveillance is agreed by the Chief Executive and available on the Orb. Authorising Officers should be suitably trained in terms of the requirements of the

Regulation of Investigatory Powers (Scotland) Act 2000. The Head of Service, Community Safety shall circulate to all relevant service areas any changes to the list of Council Officers designated to authorise directed surveillance.

Applicants should apply within their own line management structure unless other arrangements have been agreed or it is unreasonable or impractical in the circumstances. Authorising Officers shall not be responsible for authorising their own activities.

Authorisations must be given in writing. In urgent cases only, an Authorising Officer may approve oral applications. An application in writing indicating the reasons why an oral authorisation was sought must then be made as soon as reasonably practicable. In any case an oral authorisation will expire after 72 hours. If surveillance is to continue after the 72 hours a further application in writing must be made.

In accordance with the Code of Practice authorisations will last three 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 cancelled. All reviews must be documented using Form CEC/RIPSA/DS4 Review of Directed Surveillance, and shall also be recorded in the central register. Reviews will need to be carried out more frequently where the surveillance provides access to confidential information or involves collateral intrusion.

Each Service area 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.

Services wishing to adopt a more devolved authorisation process may do so only on the explicit approval of a written policy by the Council; all authorisations must remain within the scope of the Scottish Government's guidance on authorisation.

Risk assessment

By their 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 of the European Convention on Human Rights and the Human Rights Act 1998 (the right to respect for private and family life).

The Regulation of Investigatory Powers (Scotland) Act 2000 ('the Act') sets out the legal framework for the use of directed surveillance by public authorities (including local authorities), and establishes an independent inspection regime to monitor these activities.

Under the Act, Directed Surveillance will be a justifiable interference with an individual's human rights only if the conduct being authorised or required to take place is both necessary and proportionate, and in accordance with the law.

Complaints

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

Review

This policy shall be kept under review by the Head of Community Safety and Head of Legal, Risk and Compliance.

Policy on Covert Human Intelligence Sources

Policy on Covert Human Intelligence Sources

Policy Statement

In some circumstances, it may be necessary for the City of Edinburgh Council employees, in the course of their duties, to conceal their identity by working covertly. Alternatively there may arise situations when a local authority may covertly ask another person not employed by the authority such as a neighbour or an employee (the 'source') to obtain information about another person or persons and, without that other person's knowledge, pass on that information to the City of Edinburgh Council employees. By their nature, actions of this sort may constitute an interference with a person's right to privacy 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').

The Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) ('the Act') provides for the first time a legal framework for covert surveillance by public authorities (including local authorities) and an independent inspection regime to monitor these activities.

Whilst the Act does not impose a requirement for local authorities to seek or obtain an authorisation the City of Edinburgh Council employees however will, wherever possible, adhere to the authorisation procedure before carrying out any work with or as a Covert Human Intelligence Source (CHIS).

Authorising Officers within the meaning of this procedure shall avoid authorising their own activities wherever possible and only do so in exceptional circumstances.
An annual report will be submitted to members summarising the use of surveillance under this policy.

Scope

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 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 City of Edinburgh Council may themselves act as a source by failing to disclose their true identity in order to obtain information. Alternatively an employee of the City of Edinburgh 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 as part of their normal civic duties or contact numbers specifically set up to receive anonymous information, such as 'Crimestoppers'. However, someone might become a source as a result of a relationship with the City of Edinburgh Council that began in this way, and in such circumstances authorisation must then be sought.

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.

This procedure shall not apply to any disciplinary investigation or any activity involving the surveillance of employees of the Council, unless such surveillance directly relates to a regulatory function of the Council.

Policy content

Principles of Surveillance

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

Lawful purposes – covert surveillance shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in the Act) namely:

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

(ii) in the interests of public safety;

(iii) for the purpose of protecting public health;

(iii) for any other purpose prescribed in an order made by the Scottish Ministers

Necessity – a source shall only be utilised where there is no reasonable and effective alternative way of achieving the desired objective(s).

Proportionality – the use of a source shall be proportionate and not 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 cannot reasonably be obtained by other less intrusive 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 of the source will interfere with the privacy of persons other than the subject of the surveillance and to minimise the impact of the surveillance 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 Authorisation Process

Subject to the exceptions detailed below applications for the use or conduct of a source will be authorised at the level of Investigations Manager or Head of Service as prescribed by the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Order 2010. The current list of Council Officers designated to authorise the use of covert human intelligence sources is agreed by the Chief Executive and available on the Orb. Authorising Officers should be suitably trained in terms of the requirements of the Regulation of Investigatory Powers (Scotland) Act 2000. The Head of Service, Community Safety shall circulate to all relevant service areas any changes to the list of Council Officers designated to authorise the use of covert human intelligence sources

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

Authorising Officers should not be responsible for authorising their own activities.

Authorisations must be given in writing. In urgent cases only, an Investigations Manager or Head of Service or above may approve oral applications. An application in writing indicating the reasons why an oral authorisation was sought must then be made as soon as reasonably practicable. In any case an oral authorisation will expire after 72 hours. If a source is to continue to be used after the 72 hours a further application in writing must be made.

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 using Form CEC/RIPSA/CHIS4 Review of the Use of Conduct of Covert Human Intelligence Source. Reviews 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.

Each Service area 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.

Services wishing to adopt a more devolved authorisation process may do so only on the explicit approval of a written policy by the Council; all authorisations must remain within the scope of the Scottish Government's guidance on authorisation.

Confidential Material

Applications where a significant risk of acquiring confidential material has been identified shall always require the approval of the Chief Executive acting as Authorising Officer. In their absence a Director may deputise as Authorising Officer.

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 use of a source is both necessary and proportionate in these circumstances. In accordance with the Code of Practice such authorisations will last three months. Where any confidential material is obtained then the matter must be reported to Office of Surveillance Commissioners during their next inspection and any material obtained made available to them if requested.

Reviews may need to be carried out more regularly than monthly where the source provides access to confidential material, or where collateral intrusion exists.

Relationship with the Surveillance Procedure

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

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" (para 4.13). 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 acting as Authorising Officer. In their absence a Director may deputise as Authorising Officer. **Prior to deciding whether or not to grant such approval the Chief Executive, or in their absence a Director nominated to deputise, 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 12 months, excepting any authorisation involving a Juvenile CHIS which shall last only one 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 **or in their absence a Director nominated to deputise and only with the prior advice of the Chief Social Work Officer as described above.** 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 between any meetings between the authority and a source under 16 years of age

The maximum authorisation period that can be granted for a juvenile or vulnerable source is one month.

Documents

This procedure uses the following documents that shall be used by all Service areas:

Application for Authorisation of the Use or Conduct of a Covert Human Intelligence Source (Form CEC/RIPSA/CHIS1)

The applicant in all cases should complete this including where oral authorisation was first sought. It is effective from the time that approval is given.

Application for Renewal of the Use or Conduct of a Covert Human Intelligence Source (Form CEC RIPSA/CHIS2)
This should be completed where a renewal for authorisation is applied for.

Cancellation of the use or Conduct of a Covert Human Intelligence Source (Form CEC/RIPSA/CHIS3)
The applicant and the Authorising Officer should complete this when the authorisation ceases to be either necessary or appropriate.

Review of the Use or Conduct of a Covert Human Intelligence Source (Form CEC/RIPSA/CHIS4
The Authorising Officer shall complete this when carrying out reviews of authorisations

Additional Sheet for Authorising Officers to complete if required (Form EC/RIPSA/AS1)

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
- 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
(x) any relevant investigating authority other than the authority maintaining the records

Security and Retention of Documents and Materials

Documents created under this procedure are highly confidential and shall be treated as such. Service areas 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.
In addition each Service area shall also ensure arrangements are in place for the handling, storage and destruction of material obtained through directed surveillance in accordance with the requirements of the Data Protection Act 1998 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. The material must be retained until its review suggests that the risk of legal proceedings no longer exists or having taken place has now been resolved.

Central Register

The Head of Legal, Risk and Compliance shall maintain a register of current and past authorisations and of any applications for authorisations that have been refused. Each Service area will provide Legal Services with all original documentation relating to authorisations under the Regulation of Investigatory Powers (Scotland) Act 2000 including cancellations, renewals and reviews within three working days of the action being taken. Authorising Officers shall ensure that sufficient information is provided to keep this up to date.

Each authorisation will be given a unique reference number prefaced by a Service area number in brackets. The central register will contain the following information:

- Type of authorisation e.g. Directed Surveillance or Covert Human Intelligence Source
- Start date of the authorised activity
- Whether the application was authorised or refused
- Date of authorisation / refusal
- Name and Title of the Authorising Officer
- Title of the investigation or operation, if known including a brief description and names of subjects
- Whether the urgency provisions were used and if so why
- Confirmation that the Authorising Officer did not authorise their own activities
- Date of review
- Date of renewal and who authorised the renewal
- Date of cancellation
- Whether the investigation is likely to result in obtaining confidential information as defined in the Code of Practice
- Whether in the case of a CHIS the source is a juvenile or “vulnerable” person as defined in the Code of Practice

The Head of Legal, Risk and Compliance will provide regular monitoring information to Service areas.

The central register records must be retained for a period of at least three years from the ending of the authorisation or for a further suitable period if relevant to pending court proceedings.

Oversight

The Office of Surveillance Commissioners (OSC) 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 OSC.

Equalities and Rights Impact Assessment

A full Equalities and Rights Impact Assessment has been carried out in respect of this policy, and is available on request. There was no resulting indication of unlawful practice or violation of rights.

Strategic Environmental Assessment

This policy has no relevance to environmental issues and therefore an assessment is not practical.

Implementation

This policy will be implemented by each service area. Appropriate briefings shall be carried out. Authorising Officers shall be trained appropriately.

The success of the policy will be measured against a positive outcome in any statutory inspection of the Council.

Authorisation process

Subject to the exceptions detailed below, applications for the use or conduct of a source will be authorised at the level of Investigations Manager or Head of Service, as prescribed by the Regulation of Investigatory Powers (Prescription of Offices, Ranks and Positions) (Scotland) Order 2010. The current list of Council Officers designated to authorise the use of covert human intelligence sources is agreed by the Chief Executive and available on the Orb. Authorising Officers should be suitably trained in terms of the requirements of the Regulation of Investigatory Powers (Scotland) Act 2000. The Head of Service, Community Safety shall circulate to all relevant service areas any changes to the list of Council Officers designated to authorise the use of covert human intelligence sources

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

Authorising Officers should not be responsible for authorising their own activities.

Authorisations must be given in writing. In urgent cases only, an Investigations Manager or Head of Service or above may approve oral applications. An application in writing indicating the reasons why an oral authorisation was sought must then be made as soon as reasonably practicable. In any case an oral authorisation will expire after 72 hours. If a source is to continue to be used after the 72 hours a further application in writing must be made.

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 using Form CEC/RIPSA/CHIS4 Review of the Use of Conduct of Covert Human Intelligence Source. Reviews 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.

Each Service area 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.

Services wishing to adopt a more devolved authorisation process may do so only on the explicit approval of a written policy by the Council; all authorisations must remain within the scope of the Scottish Government's guidance on authorisation.

Complaints

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

Review

This policy shall be kept under review by the Head of Community Safety and Head of Legal, Risk and Compliance.

Policy on the Acquisition of Communications Data

Policy on Directed Surveillance

Policy statement

In some circumstances, it may be necessary for the City of Edinburgh Council ('the Council'), in the course of its duties, to obtain information about use of communications media by certain people.

The Regulation of Investigatory Powers Act 2000 ('the Act') sets out the legal framework for the acquisition and disclosure of communications data by public authorities (including local authorities), and establishes an independent inspection regime to monitor these activities.

The Council will adhere to the authorisation procedure described in this document.

Scope

This procedure applies in all cases where the acquisition of communications data, using the powers set out in the Act, is being planned or carried out.

The Act provides that only 'service use information' and 'subscriber information' may be applied for by a local authority. 'Traffic data' may not be obtained by a local authority under the Act.

Definitions

The Act defines 'communications data' to embrace the 'who', 'when' and 'where' of a communication, but not the 'what' (i.e. the content). It includes the manner in which, and by what method, a person or machine communicates with another person or machine. It excludes what they say or what data they pass on within a communication, including text, audio and video.

The Act defines communications data in three groups:

(a) 'traffic data' – information about where the communications are made or received;

(b) ‘service use information’ – including details of telephone numbers called and the duration of those calls; and
(c) ‘subscriber information’ – including information such as name and address of the registered user of a telephone number.

Policy content

In planning and carrying out the acquisition of communications data, Council employees shall comply with the following principles:

Lawful purposes

The Act stipulates that conduct to be authorised or required must be necessary for the purpose of preventing or detecting crime or of preventing disorder.

Any application must demonstrate that, for the relevant investigation, obtaining the requested data is:

- Necessary (for example, to investigate a suspected crime or disorder); and
- Proportionate to what is sought to be achieved (balancing the seriousness of the intrusion into privacy against the seriousness of the offence, and whether the information can be obtained by other means).

Collateral Intrusion

The application must also consider collateral intrusion. This means that consideration must be given to any actual or potential infringement of the privacy of individuals who are not the subject of the investigation or operation.

Additional Safeguard

No council employee shall obtain or any attempt to obtain ‘traffic data’ or any information about the content of any communication. Any breach of this principle may be considered a breach of the Discipline Code.

Related Documents

Applicants must use the Application for Directed Surveillance as published on the ORB and no other form. The applicant should complete this in all cases, including where oral authorisation was first sought.

A Single Point of Contact (SPoC) is accredited and trained to facilitate lawful acquisitions of communications data and effective cooperation between the Council and communications service providers. After submission of an application to the SPoC, all relevant documents are retained securely by the SPoC.

All relevant forms and guidance are published on the Orb and can be found by using the link below.

https://orb.edinburgh.gov.uk/info/200698/staff_tools/498/ripsaripa/2

Security and Retention of Documents and Materials

Documents created under this procedure are highly confidential and shall be treated as such. Service areas 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.

In addition each Service area shall also ensure arrangements are in place for the handling, storage and destruction of material obtained in accordance with the requirements of the Data Protection Act 1998 and the Code of Practice.

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

Equalities and Rights Impact Assessment

A full Equalities and Rights Impact Assessment has been carried out in respect of this policy, and is available on request. There was no resulting indication of unlawful practice or violation of rights.

Strategic Environmental Assessment

This policy has no relevance to Environmental issues and therefore an assessment is not practical.

Implementation

This policy will be implemented by each service area. Appropriate briefings shall be carried out. Designated Persons and Single points of contact shall be trained appropriately.

The success of the policy will be measured against a positive outcome in any statutory inspection of the Council.

Authorisation process

The acquisition and disclosure of communications data shall be authorised in accordance with the procedures set out in the Act.

In accordance with the Act, applications for the acquisition of communications data will be authorised by persons designated by the Council to grant authorisations ('Designated Persons'). Designated Persons are individuals holding such offices, ranks or positions as are prescribed by the Regulation of Investigatory Powers (Communications Data) Order 2010.

The current list of Council officers designated to authorise the acquisition of communications data is approved by the Chief Executive and published in the ORB. No other council officer may authorise activity under this Act.

Designated Persons should be suitably trained in terms of the requirements of the Act. The Head of Community Safety shall circulate to all relevant Service areas any changes to the list of Council officers designated to authorise the Directed Surveillance.

Designated Persons shall assess necessity and proportionality in considering whether to authorise an application.

Authorised applications will then be submitted to the Single Point of Contact (SPoC). A SPoC is accredited and trained to facilitate lawful acquisitions of communications data and effective cooperation between the Council and communications service providers.

A court order must be obtained from a Sheriff approving the grant or renewal of an authorisation before the Council can acquire communications data. If the Sheriff is satisfied that the statutory tests have been met and that the use of the technique is necessary and proportionate, he/she will issue an order approving the grant or renewal for the use of the technique as described in the application. The Council cannot acquire the communications data without such approval from a Sheriff.

Applicants should consult the Orb for guidance before making an application under the Act (https://orb.edinburgh.gov.uk/info/200698/staff_tools/498/ripsaripa/2)

Applications must be made in writing. In urgent cases only, a designated person may approve oral applications. A written application indicating the reasons why an oral authorisation was sought must then be made as soon as reasonably practicable, and within one working day.

In accordance with the Code of Practice, authorisations will remain valid for a maximum of one month from the date the Sheriff made an order approving the grant of the authorisation.

All authorisations and notices shall refer to the acquisition or disclosure of data relating to a specific time period. This specified period should be the shortest in which the objective for which the data is sought may be achieved.

The Interception of Communications Commissioner ('the Commissioner') provides independent oversight of the use of the powers contained within the Act. This oversight may include inspection visits by Inspectors appointed by the Commissioner.

Risk assessment

By their 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 of the European Convention on Human Rights and the Human Rights Act 1998 (the right to respect for private and family life).

The Regulation of Investigatory Powers Act 2000 ('the Act') sets out the legal framework for the acquisition and disclosure of communications data by public authorities (including local authorities), and establishes an independent inspection regime to monitor these activities (see above).

The acquisition of communications data under the Act will be a justifiable interference with an individual's human rights only if the conduct being authorised or required to take place is both necessary and proportionate, and in accordance with the law.

The Act imposes a requirement for local authorities to obtain an authorisation before applying for the acquisition of communications data.

Complaints

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

Review

This policy shall be kept under review by the Head of Community Safety and Head of Legal, Risk and Compliance.