Policy and Sustainability Committee

10.00am, Tuesday 30 August 2022

Regulation of Investigatory Powers (Scotland) Act 2000: Outcome of IPCO Audit and General Update

Executive/routine	**Executive**
Wards	**All**
Council Commitments	

1. Recommendations

1.1 The Policy and Sustainability Committee is asked to:

1.1.1 Note the positive outcome of the IPCO inspection; and

1.1.2 Agree the proposed revised policies on Directed Surveillance and the use of Covert Human Intelligence Sources.

Andrew Kerr

Chief Executive

Contact: Andrew Mitchell, Head of Regulatory Services

E-mail: andrew.mitchell@edinburgh.gov.uk | Tel: 0131 469 5822

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Report

Regulation of Investigatory Powers (Scotland) Act 2000: Outcome of IPCO Audit and General Update

2 Executive Summary

2.1 This report provides Committee with an update on the outcome of an inspection by the Investigatory Powers Commissioner's Office (IPCO), which took place on 22 February 2022, with respect to surveillance powers and their use by the Council. The inspection found that the Council had discharged all recommendations from previous inspection reports and had a high standard of compliance with its duties under the Act. Minor amendments reflecting corporate structure changes have been made to policies on Directed Surveillance and the use of Covert Human Intelligence Sources, and Committee is also asked to approve the revised policies.

3 Background

3.1 Local authorities in Scotland are included in the list of public bodies which may utilise the relevant provisions of the Regulation of Investigatory Powers (Scotland) Act 2000 ('RIPSA'/'the Act'). The Act provides a framework for carrying out covert surveillance activity to ensure compliance with the Human Rights Act 1998.

3.2 The Council is required to have in place policies and procedures to manage any use of surveillance. It has adopted two policies on the use of surveillance and has appointed a Senior Responsible Officer ('SRO') (the Service Director Legal and Assurance) for all activity relevant to use of the Act. The SRO is supported by the Head of Regulatory Services, who acts as RIPSA Coordinator and undertakes audit, training and policy work.

3.3 Responsibility for the Central Register of Authorisations also sits with the Service Director Legal and Assurance. Legal Services discharge the statutory function of keeping the Central Register, as well as providing feedback on quality and legal issues.

3.4 Historically the provisions of the Act were most commonly used in connection with the Council's various regulatory functions. Three service areas make active use of the Act: Planning and Transport, Regulatory Services and Family Household and Support. The levels of activity authorised have continued to decrease year on year. The Council authorised the use of 'Directed Surveillance' five times in the financial year 2016/17

and three times between January 2019 and December 2020. Brief details of this activity were provided in this Committee's business bulletin in October 2021.

3.5 The Act provides for oversight of public bodies by the Investigatory Powers Commissioner's Office (IPCO), a statutory body which oversees use of powers within the Act. IPCO previously inspected the Council in January 2019. The latest inspection took place on 22 February 2022 and was the eighth inspection of the Council. The report from this inspection (Appendix 1) became available in March 2022.

4 Main report

Use of Surveillance

4.1 Corporate use of the provisions of the Act is currently low. The Council used Directed Surveillance three times between January 2019 and December 2020 and made no use of Covert Human Intelligence Sources ('CHIS') during that period. The pandemic has meant that services, which might use these powers, have been focused on measures to protect public health and therefore were not in a position to undertake investigations which required the use of surveillance.

4.2 At its peak, the number of authorisations for the Council was 307 during 2005/06. Nationally, the use of these powers by local authorities continues to drop. In England and Wales the equivalent statutory provisions are now significantly more onerous on local authorities, and as a result surveillance by councils in England and Wales has reportedly, to a large extent, ceased.

2022 IPCO Inspection Findings

4.3 The inspection found that all recommendations from the 2019 inspection had been implemented in full and were therefore discharged.

4.4 The inspection report included the following highlights and conclusions:

4.4.1 (the inspection) "highlighted as very good practice the quality assurance process in place";

4.4.2 (there are) "suitably strong governance processes in place within your Council to ensure compliance with the legislation and Codes of Practice";

4.4.3 (Training provision) "demonstrates a real commitment on the part of the Council in ensuring staff are best prepared for conducting covert activity in a compliant and lawful manner"; and

4.4.4 "your RIPSA policies covering the use of CHIS and covert surveillance, including the guidance on the use of social media and open source research, are completely appropriate for the activity you undertake".

4.5 The inspection resulted in some observations:

4.5.1 "…policies may benefit from signposting staff to relevant sections within the Codes of Practice that provide operational examples to key elements around CHIS and online surveillance"; and

4.5.2 "With regard to the use of the internet and social media as an investigative resource, it is critical such use is appropriately overseen and audited …whether it can be afforded the protection of RIPSA or not".

Internal monitoring of activity

4.6 The RIPSA coordinator continues to monitor corporate activity through regular meetings, in addition to reviewing issues identified by Legal Services who keep the Central Register.

Training

4.7 After the 2019 IPCO inspection, the Council committed to arranging refresher training for all relevant staff.

4.8 An external provider was procured to develop a training resource, and the programme was rolled out to approximately 280 members of staff in summer 2021.

Codes of Practice

4.9 There is a requirement within the statutory Codes of Practice ('Codes') to report to members on an annual basis. Members are asked to note this report and the IPCO report attached at Appendix 1, which discharges this requirement for 2022. The previous update to members was in October 2021.

Proposed policy amendment

4.10 As a result of changes to the corporate leadership structure, the opportunity has been taken to revise and make minor changes to existing policies on Directed Surveillance and use of CHIS. Committee is asked to approve the drafts attached at Appendices 2 and 3. There are no substantive changes to the polices and any changes are restricted to updating references to job titles.

5 Next Steps

5.1 The Inspector made a number of observations, which will be implemented as appropriate.

5.2 An Integrated Impact Assessment will be completed with respect to the policies on Directed Surveillance and use of CHIS, to ensure full legal compliance, and that equality, human rights and socioeconomic disadvantage (poverty) implications are taken into account when decisions are made.

6 Financial impact

6.1 None.

7 Stakeholder/Community Impact

7.1 Use of the policies is directly relevant to the Human Rights Act 1998. Council policies have been written to ensure a high level of consideration of the impact of surveillance when carrying out public task activities.

7.2 Failure to comply with the Act and associated guidance presents a risk of legal action being taken for breach of the Human Rights Act 1998.

7.3 The Council's regulatory functions could be hampered if evidence is gathered without proper authorisation under RIPSA. There is a significant reputational risk for the Council in the use of these powers and there continues to be a high level of scrutiny from the media and public.

7.4 The attached policies set out how risks are managed. Risks are therefore mitigated by policy and training of staff.

8 Background reading/external references

8.1 Regulation of Investigatory Powers (Scotland) Act 2000: Outcome of IPCO Audit and General Update, report to Corporate Policy and Strategy Committee, 14 May 2019

9 Appendices

9.1 Appendix 1 - Letter and report from IPCO – RIPSA inspection 2022

9.2 Appendix 2 – Revised Directed Surveillance Policy for approval

9.3 Appendix 3 – Revised Covert Human Intelligence Source Policy for approval

IPCO
Investigatory Powers Commissioner's Office

PO Box 29105, London
SW1V1ZU

Mr Andrew Kerr
Chief Executive
Edinburgh City Council
4 Market Street
Edinburgh
EH8 8BG

Chief.Executive@edinburgh.gov.uk

3 March 2022

Dear Chief Executive,

IPCO Surveillance and CHIS Inspection of Edinburgh City Council

Please be aware that IPCO is not a "public authority" for the purpose of the Freedom of Information (Scotland) Act (FOISA) and therefore falls outside the reach of the FOISA. It is appreciated that local authorities are subject to the FOISA and that they may receive requests for disclosure of our reports. In the first instance the SRO should bring the matter to the attention of the IPCO Data Protection Officer (at: info@ipco.org.uk), before making any disclosure. This is also the case if you wish to make the content of this letter publicly available.

Your authority was recently subject to a remote inspection by one of my Inspectors, Mr. Paul Donaldson. The documentation and arrangements necessary for my Inspector to carry out the process was provided by Mr. Andrew Mitchell, Head of Regulatory Services, who acts as your RIPSA Coordinator. This enabled an examination of relevant policies and four of the directed surveillance authorisations granted since the last inspection in January 2019. Mr. Mitchell, along with Mr. Nick Smith, Head of Legal and Assurance who acts as your Senior Responsible Officer (SRO), Mr. Kevin McKee, Head of Legal Service, and Mr. Keith Irwin, Principal Solicitor, made themselves available to be interviewed via video conferencing, and from the documentation examined and the information provided during the interview the level of compliance shown by your authority removes, for the present, the requirement for a physical inspection.

At the last inspection your authority was subject to two recommendations, and I note that in response to these and some observations made, a comprehensive action plan was devised to monitor progress to ensure they were appropriately addressed. From the information provided, in response to Recommendation 1 a process has now been established to report RIPSA matters to Elected Members who sit on the Council's Corporate Policy and Sustainability Committee, as required by paragraphs 4.43[1] and 3.27[2]. I understand there had been a hiatus during the pandemic, but since late 2021 these reports are once again to be delivered to the Committee.

[1] Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017
[2] Scottish Government Code of Practice on Covert Human Intelligence Sources, December 2017

In respect of Recommendation 2, a training needs analysis has been completed to identify the training required for staff and, as well as the ongoing delivery of an in-house online refresher training package to over 300 staff, the Council has also, to some expense, procured an external provider to provide a bespoke course to relevant investigative staff. This demonstrates a real commitment on the part of the Council in ensuring staff are best prepared for conducting covert activity in a compliant and lawful manner.

My Inspector has expressed confidence that your RIPSA policies covering the use of CHIS and covert surveillance, including the guidance on the use of social media and open source research, are completely appropriate for the activity you undertake. Mr. Donaldson has highlighted that the policies may benefit from signposting staff to relevant sections within the Codes of Practice[3] that provide operational examples to key elements around CHIS and online surveillance. Whilst there has been no use of CHIS, providing guidance to staff around situations where potential considerations of CHIS may be necessary is crucial. Paragraphs 2.18, 2.23 and 2.25[4], may be useful to Council staff who may interact with members of the public who offer information, particularly those who do so repeatedly, and where it may be necessary for them to consider the guidance on CHIS.

With regard to the use of the internet and social media as an investigative resource, it is critical such use is appropriately overseen and audited within all public authorities, whether it can be afforded the protection of RIPSA or not. In that regard my Inspector discussed The Investigatory Powers Tribunal's (IPT) decision in *BA & others v Chief Constable of Cleveland IPT/11/129/CH (13 July 2012)* where the IPT commended the adoption in non-RIPA (RIPSA) cases "a procedure as close as possible" to that required by the legislation. It was highlighted that in some areas of the Council, records of online activity are maintained for auditing purposes, which I would commend as being good practice. This serves to reduce the risk of there being any disproportionate use of social media and ensure legitimate aims are being pursued through its use. I note that the external training being procured contains relevant material on the deployment of such activity.

Mr. Donaldson examined four directed surveillance authorisations granted since the last inspection and makes the following points:

1. The Applicant and Authorising Officer (AO) provided sufficient and specific background information on the investigation which allowed the requisite elements of necessity, proportionality, and collateral intrusion to be considered as per paragraph 5.4[5].

2. Whilst the relevant content is present, it seems applicants at times will conflate considerations attached to necessity and proportionality. Applicants should focus on the elements of proportionality contained within paragraph 4.7[6].

3. AOs set appropriate review dates and the contents of reviews allow for an assessment of the continued necessity and proportionality of the authorised activity as per paragraph 8.11[7].

4. AOs should ensure their authorisations are maintained in accordance with paragraphs 5.19 to 5.21[8] and Chapter 8 of the Code of Practice. Cancellations should provide detail on what activity has been undertaken, the type and extent of the product and material obtained, and how it is to be managed, with the AO providing some direction or instruction for its management.

---

[3] Scottish Government Codes of Practice on Covert Surveillance and Property Interference, December 2017 paras 3.11 to 3.16 and Covert Human Intelligence Sources paragraphs 4.7 to 4.14
[4] Scottish Government Code of Practice on Covert Surveillance and Property Interference, December 2017
[5] Ibid
[6] Ibid
[7] Ibid
[8] Ibid

Mr. Donaldson has highlighted as very good practice the quality assurance process in place where applications and authorisations are reviewed by Legal Services, although in one case it seems to have taken place post-authorisation where the pertinent comments could arguably have necessitated a review being submitted. Whilst quality assurance is good practice, it would be more appropriate always to take place prior to submission to the AO and to include any guidance to the AO as is necessary.

I am aware that since the last inspection you have received my letter outlining IPCO's recent Data Assurance Programme and that both your policies contain sections dedicated to *Security and Retention of Documents and Materials* which provide some guidance on the retention, review and disposal of material obtained through covert activity. My Inspector has made the observation that it would be beneficial for this guidance to be aligned with the content of the relevant Codes of Practice and with the principles outlined in my aforementioned letter.

I am pleased to report there being suitably strong governance processes in place within your Council to ensure compliance with the legislation and Codes of Practice. I would highlight that the observations made herein are designed to assist your staff in their respective roles should they need to utilise covert investigative techniques.

I hope that you find the outcome of this remote inspection helpful and constructive, and my Office is available to you should you have any queries following the receipt of this letter, or at any point in the future. Contact details are provided below. I shall in any case, be interested to learn of your proposed response to any of the observations made within this letter within the next two months.

The Inspector would like to thank Mr. Andrew Mitchell for his positive engagement with the remote inspection process, and for providing the necessary documentation to enable it to be achieved.

Yours sincerely,

[redacted]

The Rt. Hon. Sir Brian Leveson
The Investigatory Powers Commissioner

Appendix 2

Policy on Directed Surveillance

1 Policy Statement

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 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).

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

1.3 Whilst RIPSA does not impose a requirement for local authorities to seek or obtain an authorisation, Council employees will, wherever possible, adhere to the authorisation procedure before conducting any covert surveillance.

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

1.5 No activity shall be undertaken by Council employees that comes within the definition of 'Intrusive Surveillance'. Intrusive surveillance is covert surveillance of any activity 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.

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

2 Scope

2.1 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).

2.2 The procedure does not apply to:

2.2.1 observations that are carried out overtly;

2.2.2 unplanned observations made as an immediate response to events where it was not reasonably practicable to obtain authorisation;

2.2.3 non-planned, ad hoc covert observations that do not involve the systematic surveillance for a specific investigation or operation; or

2.2.4 any disciplinary investigation or any activity involving the surveillance of Council employees, unless such surveillance directly relates to a regulatory function of the Council.

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

2.4 The objective of this procedure is to ensure that all covert surveillance by 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 and Property Interference, issued on 11 December 2017 (the "Code of Practice") and any guidance which the Investigatory Powers Commissioner's Office 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.

2.5 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.

2.6 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.**

2.7 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 (i) a Council Authorising Officer or, (ii) 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. Reference should be made to the Council's policy on use of CCTV.

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

3 Definitions

3.1 "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.

3.2 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.

4 Policy content

4.1 Principles of Surveillance

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

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

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

(ii) in the interests of public safety; or

(iii) for the purpose of protecting public health.

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

4.1.3 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

4.1.4 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.

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

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

4.2 The Authorisation Process

4.2.1 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, etc. and Specification of Public Authorities) (Scotland) Order 2010 (as amended) ('the 2010 Order').

4.2.2 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 RIPSA. The Council's RIPSA Coordinator shall circulate to all relevant service areas any changes to the list of Council Officers designated to authorise directed surveillance.

4.2.3 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.

4.2.4 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.

4.2.5 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.

4.2.6 Each Service area will keep an appropriate record of any application made. Any refusal shall be recorded in the Central Register.

4.2.7 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.

4.2.8 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 Code of Practice on authorisation.

4.3 Confidential Material

4.3.1 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 an Executive Director may deputise as Authorising Officer.

4.3.2 Confidential material consists of:

4.3.2.1 matters subject to legal advice privilege (for example between professional legal adviser and client) or litigation privilege.

4.3.2.2 confidential personal information (for example relating to a person's physical or mental health) or

4.3.2.3 confidential journalistic material.

4.3.3 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 the Investigatory Powers Commissioner's Office during their next inspection and any material obtained made available to them if requested.

4.4 **Documents**

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

4.4.1 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.

4.4.2 Application for Renewal of Directed Surveillance Authority (Form CEC RIPSA/DS2)

This should be completed where a renewal of authorisation is applied for.

4.4.3 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.

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

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

4.5 **Security and Retention of Documents and Materials**

4.5.1 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 2018 and the Code of Practice.

4.5.2 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 2018 and the Code of Practice.

4.5.3 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.

4.6 Central Register

4.6.1 The Service Director Legal & Assurance 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 RIPSA, 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.

4.6.2 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:

- 4.6.2.1 type of authorisation e.g. Directed Surveillance or Covert Human Intelligence Source;
- 4.6.2.2 start date of the authorised activity;
- 4.6.2.3 whether the application was authorised or refused;
- 4.6.2.4 date of authorisation / refusal;
- 4.6.2.5 name and title of the Authorising Officer;
- 4.6.2.6 title of the investigation or operation, if known, including a brief description and names of subjects;
- 4.6.2.7 whether the urgency provisions were used and, if so, why;
- 4.6.2.8 confirmation that the Authorising Officer did not authorise their own activities;
- 4.6.2.9 date of review;
- 4.6.2.10 date of renewal and who authorised the renewal;
- 4.6.2.11 date of cancellation; and
- 4.6.2.12 whether the investigation is likely to result in obtaining confidential information as defined in the Code of Practice.

4.6.3 The Service Director Legal & Assurance will provide regular monitoring information to Service areas.

4.6.4 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.

5. Oversight

5.1 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 RIPSA. This oversight includes inspection visits by Inspectors appointed by IPCO.

6. Equalities and Rights Impact Assessment

6.1 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

7. Strategic Environmental Assessment

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

8. Implementation

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

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

9 Authorisation process

9.1 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 2010 Order. 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 RIPSA. The RIPSA Coordinator shall circulate to all relevant service areas any changes to the list of Council Officers designated to authorise directed surveillance.

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

9.3 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.

9.4 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.

9.5 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.

9.6 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.

9.7 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.

10 Risk assessment

10.1 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).

10.2 RIPSA 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.

10.3 Under RIPSA, 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.

11 Complaints

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

12 Review

12.1 This policy shall be kept under review by the Service Director Legal & Assurance.

Appendix 3

Policy on Covert Human Intelligence Sources

1 Policy Statement

1.1 In some circumstances, it may be necessary for Council employees, in the course of their duties, to conceal their identity by working undercover. Alternatively, there may arise situations when a local authority may covertly ask another person not employed by the authority, such as a neighbour (the 'source'), to obtain information about another person or persons and, without that other person's knowledge, pass on that information to 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').

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

1.3 Whilst RIPSA does not impose a requirement for local authorities to seek or obtain an authorisation, 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').

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

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

2 Scope

2.1 This procedure applies in all cases where a CHIS is to be used. CHIS 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.

2.2 A local authority may therefore use a source in two main ways. Council employees may themselves act as a source by failing to disclose their true identity in order to obtain information. Alternatively, Council employees 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.

2.3 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 Council that began in this way, and in such circumstances authorisation must then be sought.

2.4 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.

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

3 Policy content

3.1 Principles of Surveillance

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

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

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

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

3.1.3 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

3.1.4 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.

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

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

4 Authorisation Process

4.1 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, etc. and Specification of Public Authorities) (Scotland) Order 2010 (the "2010 Order"). 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 RIPSA. The RIPSA Coordinator 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.

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

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

4.4 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.

4.5 In accordance with the Scottish Government Code of Practice on Covert Human Intelligence Sources, issued on 11 December 2017(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.

4.6 Each Service area will keep an appropriate record of any application made. Any refusal shall be recorded in the Central Register.

4.7 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.

4.8 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 Code of Practice on authorisations.

5 Confidential Material

5.1 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, an Executive Director may deputise as Authorising Officer.

5.2 Confidential material consists of:

5.2.1 matters subject to legal advice privilege (for example between professional legal adviser and client) or litigation privilege;

5.2.2 confidential personal information (for example relating to a person's physical or mental health); or

5.2.3 confidential journalistic material.

5.3 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 para 5.14 of the Code of Practice such authorisations will last twelve months (except in the case of (i) a juvenile CHIS or (ii) matters pertaining to the 2014 Order[1]), namely any authorisation relating to paragraph 5.2.1 above.

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

6 Relationship with the Surveillance Procedure

6.1 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.

[1] The Regulation of Investigatory Powers (Authorisation of Covert Human Intelligence Sources) (Scotland) Order 2014

6.2 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.

6.3 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.

7 Vulnerable and Juvenile Sources

7.1 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 4.1). 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 an Executive Director may deputise as Authorising Officer. **Prior to deciding whether or not to grant such approval the Chief Executive, or in their absence an Executive 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.

7.2 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.

7.3 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 Executive 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:

7.3.1 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;

7.3.2 the Authorising Officer must be satisfied that any risks have been properly explained; and

7.3.3 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.

7.4 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.

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

8 Documents

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

8.1.1 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.

8.1.2 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.

8.1.3 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.

8.1.4 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.

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

9 Management of Sources

9.1 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:

9.1.1 dealing with the source on behalf of the authority;
9.1.2 directing the day to day activities of the source;
9.1.3 recording the information supplied by the source; and
9.1.4 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.

9.2 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.

9.3 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:

9.3.1 identity of the source and the means by which the source is referred to;
9.3.2 the date when and the circumstances within the source was recruited;
9.3.3 the name of the person with day to day responsibility for the source and the name of the person responsible for overall oversight;
9.3.4 any significant information connected with the security and welfare of the source;
9.3.5 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;
9.3.6 all contacts between the source and the local authority;
9.3.7 any tasks given to the source;
9.3.8 any information obtained from the source and how that information was disseminated;
9.3.9 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
9.3.10 any relevant investigating authority other than the authority maintaining the records.

10 Security and Retention of Documents and Materials

10.1 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 2018 and the Code of Practice.

10.2 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 2018 and the Code of Practice.

10.3 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.

11 Central Register

11.1 The Service Director Legal & Assurance shall maintain a register of current and past authorisations and of any applications for authorisations that have been refused, in accordance with para 7.1 of the Code of Practice. Each Service area will provide Legal Services with all original documentation relating to authorisations under RIPSA 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.

11.2 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:

- 11.2.1 type of authorisation e.g. Directed Surveillance or Covert Human Intelligence Source;
- 11.2.2 start date of the authorised activity;
- 11.2.3 whether the application was authorised or refused;
- 11.2.4 date of authorisation / refusal;
- 11.2.5 name and Title of the Authorising Officer;
- 11.2.6 title of the investigation or operation, if known including a brief description and names of subjects
- 11.2.7 whether the urgency provisions were used and if so why;
- 11.2.8 confirmation that the Authorising Officer did not authorise their own activities;
- 11.2.9 date of review;
- 11.2.10 date of renewal and who authorised the renewal
- 11.2.11 date of cancellation;
- 11.2.12 whether the investigation is likely to result in obtaining confidential information as defined in the Code of Practice; and
- 11.2.13 whether in the case of a CHIS the source is a juvenile or “vulnerable” person as defined in the Code of Practice.

11.3 The Service Director Legal & Assurance will provide regular monitoring information to Service areas.

11.4 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

12 Oversight

12.1 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 RIPSA. This oversight includes inspection visits by inspectors appointed by IPCO.

13 Equalities and Rights Impact Assessment

13.1 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

14 Strategic Environmental Assessment

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

15 Implementation

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

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

16 Authorisation process

16.1 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 RIPSA. The RIPSA Coordinator 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

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

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

16.4 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.

16.5 In accordance with the Code of Practice, authorisations will last 12 months, or one month for a vulnerable or juvenile CHIS (para 4.2). 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.

16.6 Each Service area will keep an appropriate record of any application made. Any refusal shall be recorded in the Central Register.

16.7 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.

16.8 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 Code of Practice.

17 Complaints

17.1 RIPSA establishes an independent Tribunal with 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 RIPSA. Details of the relevant complaints procedure can be obtained from the Investigatory Powers Tribunal, PO Box 33220, London, SW1H 9ZQ.

18 Review

18.1 This policy shall be kept under review by the Service Director Legal & Assurance .