Corporate Policy and Strategy Committee

10.00am, Tuesday, 14 May 2019

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

Item number	
Executive/routine	
Wards	All
Council Commitments	N/A

1. Recommendations

It is recommended that the Corporate Policy and Strategy Committee:

1.1 notes the positive outcome of the IPCO inspection;

1.2 notes that powers under the Act have not been used since 2016; and

1.3 agrees the proposed revised policies on Directed Surveillance and the use of Covert Human Intelligence Sources.

Andrew Kerr

Chief Executive

Contact: Nick Smith, Head of Legal & Risk

E-mail: nick.smith@edinburgh.gov.uk | Tel: 0131 529 4377

Contact: Andrew Mitchell, Regulatory Services Manager

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

Report

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

2. Executive Summary

2.1 This report provides members with an update on surveillance powers and the use of them by the Council, including the outcome of an inspection by the Investigatory Powers Commissioner's Office (IPCO) which took place on 24 January 2019. The inspection found that the Council had discharged all the recommendations from previous inspection reports and had a high standard of compliance with its duties under the Act. The report provides details of an action plan to address the two recommendations arising from the inspection and asks the committee to approve revised policies on Directed Surveillance and the use of Covert Human Intelligence Sources.

3. Background

3.1 Local authorities in Scotland are included within 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 Head of Legal and Risk) for all activity relevant to use of the Act. The SRO is supported by the Regulatory Services Manager, 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 Head of Legal and Risk. Colleagues within 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 made active use of the Act: Planning and Transport, Regulatory Services and Safer and Stronger

Communities. 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 none since.

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's predecessor previously inspected the Council in June 2016. The latest inspection took place on 24 January 2019 and was the seventh inspection of the Council. The report from this inspection became available in February 2019.

4. Main report

Use of Surveillance

4.1 Corporate use of the provisions of the Act is currently low, and the Council has not used Directed Surveillance or Covert Human Intelligence Sources ('CHIS') since 2016/17.

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.

2019 OSC Inspection Findings

4.3 The inspection found that all recommendations from the 2016 inspection had been implemented in full, and therefore discharged.

4.4 The inspection report included the following highlights and conclusions:

4.4.1 "This was an excellent inspection".

4.4.2 "With continued investments in training (the Inspector has) no doubt that Edinburgh City Council will continue to achieve this high-level of compliance".

4.4.3 The Inspector commented that the Council's formal recording of Legal Services reviews of authorisations "is an example of good practice that introduces extra safeguards".

4.4.4 the member awareness sessions run in 2017 were cited as a positive by the inspector.

Internal monitoring of activity

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

Codes of Practice

4.6 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 2019.

Proposed policy amendment

4.7 The Codes have been revised since previous Council policies were approved by members. As a result, the opportunity has been taken to revise and make minor changes to existing policies on Directed Surveillance and use of any CHIS. Members are asked to approve the drafts attached at Appendices 2 and 3.

4.8 Committee should note that there are no substantive changes. Any changes are restricted to updating references to named officers and reference to the creation of IPCO, which replaced the former statutory oversight body.

5. Next Steps

5.1 The Inspector made two recommendations and three observations, which will be implemented. The recommendations are detailed in the Action Plan attached at Appendix 4.

5.2 The Council has written to IPCO with confirmation that these will be implemented.

6. Financial impact

6.1 The proposed training programme shall require to be funded and is estimated to be in the range of £15 -20K, to be contained within the corporate training budget.

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 Members may be concerned at the risk of interference with the right to privacy provided for in the Human Rights Act 1988.

7.4 The Council's regulatory functions could be hampered if evidence is gathered without proper authorisation under RIP(S)A.

7.5 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.

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

8. Background reading/external references

8.1 RIPSA inspection report and update 2017

9. Appendices

9.1 Appendix 1 - Letter and report from IPCO – RIPSA inspection 2019

9.2 Appendix 2 – Revised Directed Surveillance Policy for approval

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

9.4 Appendix 4 – Action plan

OFFICIAL -SENSITIVE

IPCO
Investigatory Powers
Commissioner's Office

PO Box 29105, London
SW1V 1ZU

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

7 February 2019

Inspection of Edinburgh City Council

Dear Mr Kerr,

On 24th January 2019 one of our inspectors, Brendan Hughes, examined the arrangements made by Edinburgh City Council to secure compliance with the legislative provisions which govern the council's use of the investigatory powers under the Investigatory Powers Act (2016), the Regulation of Investigatory Powers Act (2000) and the Regulation of Investigatory Powers (Scotland) Act (2000). I have attached the report that was compiled following the inspection which I endorse.

As described by my Inspector in his conclusion, this has been an "excellent" inspection that demonstrates Edinburgh City Council has attained a high standard of compliance with the legislation and the relevant Codes of Practice and made good progress in responding to the recommendations of the previous inspection by the OSC. With the marked decline in authorisations, care must be taken to maintain this level of compliance through continued training and awareness and the SRO should pay particular attention to this area.

Mr Hughes makes two recommendations in his report. I would be grateful if you could acknowledge these and respond to me within two months of the receipt of this letter with details of an action plan to address these recommendations. He has also advanced a number of observations that I am confident will assist your staff, to which I am sure you will give careful consideration.

I trust that this Report will not discourage your staff from utilising these important powers, which enable your authority to investigate and combat crime. Indeed, I can foresee a time when there may be understandable public concern if the decline across the United Kingdom continues in the use of some of these highly useful investigative techniques.

In the meantime, please do not hesitate to contact my office should you require any further assistance.

Yours sincerely

[redacted]

The Rt Hon. Lord Justice Fulford
The Investigatory Powers Commissioner

0207 389 8900 info@ipco.gsi.gov.uk @IPCOffice www.ipco.org.uk

OFFICIAL-SENSITIVE

IPCO/INSP/074

IPCO
Investigatory Powers Commissioner's Office

Inspection Report – Edinburgh City Council

Contents

1 Introduction

1.1 This inspection has been conducted to assess Edinburgh City Council's level of compliance with the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A), the Regulation of Investigatory Powers Act 2000 (RIPA) and all associated Codes of Practice in respect of the Council's use of covert surveillance, covert human intelligence sources (CHIS) and requests for communications data (CD).

1.2 Edinburgh Council is one of 32 unitary local authorities in Scotland. It became a single-tier council area in 1996 following the Local Government etc. (Scotland) Act 1994. Edinburgh is the second largest city in Scotland, with an estimated population of approximately 470,000 in mid-2012. It is Scotland's capital city and home to the Scottish Parliament. As with all local authorities in Scotland, Edinburgh has had to manage significant reductions in funding through the period of inspection.

1.3 The inspection took place on 24h January 2019 and examined the period from the last inspection by the OSC, which was conducted on the 10th of June 2016. The inspection was conducted by IPCO Inspector Brendan Hughes.

1.4 This report should be addressed to:

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

2 Inspection methodology

2.1 Prior to the inspection, key policy documents were made available. During the inspection interviews were held with a wide range of key staff including the Senior Responsible Officer (SRO – Nick Smith, Head of Legal and Risk and also the Council Monitoring Officer), the RIP(S)A Co-ordinator (Andrew Mitchell, Regulatory Services Manager), two Authorising Officers (AOs - David Leslie, Chief Planning Officer and Cliff Hutt Specialist Service Manager Transport), and members of the Council's legal team (Kevin McKee, Senior Legal Manager, and Keith Irwin, Principal Solicitor).

2.2 A focus group was held with a good selection of operational-level staff from across different council departments. The Central Record of authorisations was examined as were all three applications, authorisations, reviews, renewals and cancellations made during the period of inspection. The CCTV control room was visited and a meeting was held with the Community Safety Manager and the CCTV operations supervisor.

2.3 Statistics relating to what was viewed at this inspection are captured in Table 1 below. Please see Section 7 for a full list of which records were viewed during the inspection.

Edinburgh City Council	Inspection period: 10/6/16-10/11/19					
	Total authorisations in current inspection period	Total authorisations in previous inspection period	Total records viewed at Inspection	Of this total, number of urgent oral records viewed	Of this total, number of major modifications viewed	Of this total, number of minor modifications viewed
Directed Surveillance	3	53	3	N/A	N/A	N/A
CHIS (crime)	0	0	N/A	N/A	N/A	N/A

Table 1. Key Statistics

3 Key findings

3.1 Recommendations

3.1.1 This was an excellent inspection, well facilitated by the SRO and RISP(S)A Co-ordinator. Two recommendations have been made, one of which was an issue of compliance that had already been identified by the Council and should be easily addressed.

3.1.2 The key recommendations arising from the inspection are listed in Table 2 below.

Number	Reference	In relation to	Recommendation	Recommendation type
R1	**5.7**	**Policy**	It is recommended that the council fully implement the requirement to ensure that elected representatives have the opportunity to review the council's use of RIP(S)A and set policy at least once a year	Core recommendation - improvements must be made
R2	**5.30**	**Training**	It is recommended that the council undertake a RIP(S)A training needs analysis and ensures staff receive training as identified. A central register of RIP(S)A related training should be maintained.	Recommendation - observed potential for improvements

Table 2. Key recommendations resulting from inspection

3.2 Observations

3.2.1 The key observations arising from the inspection are listed in Table 3 below.

Number	Reference	In relation to	Recommendation	Observation type
O1	5.10	Authorisation Process – Legal review	The formal recording of legal review of RIP(S)A applications prior to authorisation is an example of good practice that introduces extra safeguards.	Comment – observation or praise of good practice
O2	5.28	Policy	The council should adopt a method of indicating effective-from and version control for its RIP(S)A related policies.	Comment – observation where practice could be improved
O3	5.32	Training	The council should consider running one or more RIP(S)A authorisation exercises on an annual basis as well as instituting a RIP(S)A forum.	Comment – observation where practice could be improved

Table 3. Key observations resulting from inspection

4 Previous recommendations

4.1 The following progress was noted on recommendations made during the previous inspection:

4.2 *Recommendation 1 - The cancellations of directed surveillance authorisations by authorising officers should include the information provided by Notes 109 to 109.4 inclusive of the OSC Procedures and Guidance document.*

4.3 **Discharged**. The inspection found that of the three authorisations given, all met the minimum required, although one was notably weaker than the others. This will be commented on in more detail in the inspection findings below.

4.4 *Recommendation 2 - The council's CCTV Code of Practice should be amended to include the relevant RIPSA considerations inherent in the use of the council CCTV, and the current agreement which is in use by the council and Police Scotland to accommodate the use of the council CCTV system in connection with directed surveillance authorisations granted by the police, should similarly be updated and incorporate relevant terminology.*

4.5 **Discharged**. The CCTV Code of Practice is undergoing a significant revision at the time of inspection, principally in response to changes in data protection law. RIP(S)A requirements or considerations were not included in the new draft, but will be included in the final version. RIP(S)A is however dealt with comprehensively in the Information Sharing Agreement with Police Scotland, and that more than adequately deals with the substance of this recommendation, which can therefore be considered discharged. Further discussion on this point is set out in the inspection findings below.

4.6 *Recommendation 3 - The council should maintain a proportionate programme of staff awareness provision with regards to the responsibilities they have associated with RIPSA.*

Discharged. Subsequent to the last inspection the council undertook significant general staff training in partnership with an Edinburgh-based university. This will be discussed in more detail in the 'relevant training' section below.

4.7 *Recommendation 4 - The SRO should review the provision of the authorising officer function within the council to ensure that the legal responsibilities associated with that role may be discharged diligently and expeditiously.*

Discharged. The inspection found that the council had a sufficient number of authorising officers of sufficient knowledge, experience, rank and independence to discharge the function.

4.8 *Recommendation 5 - The council should, in consideration of both the strategic and user requirement for open source research within its investigative function, provide coherent policies, training and processes so that such activity may be conducted where necessary, lawfully and in a manner which maintains the confidence of the communities which the council serves.*

4.9 **Discharged.** The inspection found that council officers understood the risks associated with digital investigation and how on-line research can become directed surveillance and that there were adequate policy and technical safeguards in place to limit the risk of staff conducting unauthorised directed surveillance via social media.

5 Inspection findings

Errors

5.1 No errors have been reported during the period under inspection and none were found during the inspection.

Confidential Information

5.2 There has been no case where confidential information has been obtained.

Journalistic Material

5.3 No journalistic material was sought or obtained.

Legally Privileged Material

5.4 No Legally Privileged Material was sought or obtained.

Informing Elected Representatives

5.5 At the outset of the inspection the Council volunteered that they had not been able to fully comply with the requirements to keep elected members informed on an annual basis, with a hiatus in 2018. Section 4.43 of the most recent RIP(S)A Surveillance and property interference code of practice sets out the requirement:

"In addition, elected members of a local authority should review the authority's use of RIP(S)A and set the policy at least once a year. They should also consider internal reports on use of RIP(S)A on at least a quarterly basis to ensure that it is being used consistently with the local authority's policy and that the policy remains fit for purpose. They should not, however, be involved in making decisions on specific authorisations. In regard to the matters mentioned in this paragraph, local authorities may wish to consider ensuring that their elected members have undergone sufficient training in order to fulfil these requirements."

5.6 The matter was discussed in some detail. One interesting point made was that the council committees have to consider over 900 reports per annum and that councillors were not keen on receiving reports that merely stated the *status quo* or contained nothing of substance to consider. It certainly highlights the impracticality of the consideration of quarterly reports as suggested by the Codes of Practice. This is especially true for councils like Edinburgh that rarely grant authorisations. Nevertheless, an annual report should still be made and endorsement of policy (both for CHIS and surveillance) sought – it is an important part of maintaining democratic oversight and public confidence in the availability and use of these powers. It was suggested that this be synchronised with the annual statistical return to IPCO, which is now asked for on a calendar year (i.e. making the report/endorsing policy in January each year).

5.7 It should also be noted that unlike many councils, Edinburgh had invested in briefing elected members on RIP(S)A and how the techniques are used and authorised. This was examined prior to the inspection and was of very commendable detail and quality.

5.8 **Recommendation 1 (R1). It is recommended that the Council fully implement the requirement to ensure that elected representatives have the opportunity to review the Council's use of RIP(S)A and set policy at least once a year.**

Centrally Retrievable Register of Authorisations

5.9 The Centrally Retrievable Register of Authorisations was examined and met the required standard. The forms in use were tailored versions of those provided by the Scottish Government. The Council had made one significant innovation, which was to obtain a legal review of each application before it was submitted to the authorising officer, with the legal view recorded on a separate form. This was an excellent initiative, going beyond what was required by the Codes of Practice. It was clear during the inspection of actual authorisations, that this extra safeguard in the process had helped identify weakness and errors in applications. This is an example of good practice.

5.10 **Observation 1 (O1): The formal recording of legal review of RIP(S)A applications prior to authorisation is an example of good practice that introduces extra safeguards.**

Directed Surveillance

5.11 Three authorisations for Directed Surveillance had been granted during the period under inspection. All three had been made in 2016, with none subsequently. One related to the deployment of a covert CCTV camera to gather evidence of unlicensed street trading, another related to mobile surveillance to investigate fraudulent use of a disabled 'blue-badge' and the third involved the deployment of covert foot surveillance to monitor anti-social crime hotspots. All three authorisations and their associated reviews and cancellations were examined during the inspection.

5.12 This marks a very significant reduction to the previous period of inspection, which saw 53 directed surveillance authorisations (DSAs). The reasons for the reduction was discussed with the SRO, AOs and RIP(S)A co-ordinators. The reason for the reduction was two-fold: firstly, very significant budget cuts had led to a reduction in investigative capacity in some areas and secondly, more effort was made to adopt different tactics focusing on prevention rather than detection of issues. This was often also felt to be more cost-effective. Significantly, none of the staff interviewed felt that the legislation itself or the authorisation process acted as a deterrent from seeking to use the powers. This is important as it means that the necessity of obtaining an authorisation is not having an unintended 'chilling' effect, or creating an incentive for unauthorised activity.

5.13 It was emphasised in the inspection that there is no right or wrong number of authorisations and that 'league table' comparisons were meaningless as each authorisation had to be considered entirely on its own merits and circumstances. What mattered was that the Council had access to the powers when necessary and could use them in a compliant manner. Where the reduction in numbers mattered was that it could raise the risk of non-compliance through growing lack of practical experience of making and authorising applications and unfamiliarity with the authorisation process. It is the SRO's responsibility to maintain the integrity of the RIP(S)A process and one

way they could mitigate this growing risk is through continued training and exercises (discussed in more detail below).

5.14 All applications met the necessary standard, but with considerable variation in quality between the applications. Authorisation 1617/002 (the 'blue-badge' fraud) was of a very high standard which was good to see considering the complexities inherent in the conduct of mobile surveillance. The surveillance was cancelled very promptly (the same morning) after the evidence had been successfully obtained. This was a good example of best practice by the authorising officer, and very commendable. Unfortunately the Council reported it no longer has the capacity to conduct such investigations due to resource constraints following reorganisation.

5.15 Authorisation 1617/001 was less well constructed. Part of the difficulty was that the covert surveillance was simply one aspect of a broader operation to tackle very high levels of anti-social behaviour in public spaces in two wards of Edinburgh. This was well set out in the section of the application describing the context of the authorisation, but discussion of the overt elements was carried forward into the sections which should have focused solely on the covert conduct (i.e. the plain-clothes foot patrols). Also the geographical scope of the surveillance was broadly described. This in itself is not an issue if it can be shown clearly to the authorising officer that it is necessary, but a more detailed description by the applicant would have helped make the case. There is no reason why an attachment of a visual aid, such as a map, could not be attached to help the authorising officer clearly understand the scope of proposed surveillance. The discussion of collateral intrusion was not sufficiently detailed either.

5.16 All authorisations were clearly in the authorising officer's own words and all had clearly engaged with the detail of the application. All had review periods set.

5.17 Following advice from a previous OSC inspection, some sections of some authorisations had been hand written by the authorising officer, with additional comments and changes to the applications made in hand by the authorising officer. The difficulty with handwritten entries, is that AOs can restrict their comments to fit the box provided on the printed-out version of the form. Digital entries face no such restriction and IPCO now advises that it is not necessary for authorising officers to hand-write their authorisations. What matters is that once the authorisation has been granted (or rejected), it cannot be altered in anyway and its integrity is preserved. Saving the finalised MS Word form as a PDF and clearly marking it as the final version is one way to achieve this or by saving an un-editable version of the document into the Council's electronic document and record management system (EDRMS - if in use).

5.18 Ideally, authorising officers should not correct or alter the application itself, although it does show excellent engagement with the application. The authorising officer should either reject the application, if the error is serious enough, or address the issues with the application (e.g. specifying whether a covert CCTV camera is to be used for audio as well as video) in the conduct that they authorise, making sure that any variance between what was sought, and what was authorised, is clearly drawn to the attention of the applicant.

5.19 One minor issue common to all the authorisations related to the necessity test. All three authorisations provided excellent detail on why the authorisation was necessary, but failed to state clearly at the outset the statutory purpose (e.g. 'for the prevention and detection of crime'). This is possibly an artefact of the design of the standard RIP(S)A form provided by the Scottish Government, which has one box for the statutory purpose and then another for the detailed discussion of necessity.

Directed Surveillance - Noise Monitoring

5.20 In line with the Section 3.37 of the RIP(S)A Surveillance Code of Practice, Edinburgh City Council does not seek directed surveillance authorisations for the deployment of noise monitoring equipment.

Directed Surveillance – CCTV

5.21 Edinburgh City Council owns and operates a significant public-space CCTV network. The system is manned by council staff on a shift basis. A brief, but very informative, visit was made to the control room and a meeting held with the managers responsible for the operation of the CCTV system. The inspection found that excellent protocols were in place in relation to the use of CCTV by the council or third-parties such as Police Scotland for directed surveillance, with clear instructions to staff which provided a proven safeguard against non-authorised surveillance.

5.22 As mentioned above, the Council is in the process of drawing all of its CCTV related activity under a single Code of Practice. At the request of Edinburgh City Council, the draft was reviewed immediately after the inspection. In the draft provided, RIP(S)A is mentioned in the Legal Framework section, but then not referred to again, with no explanation of why RIP(S)A would be relevant to the Council's use of CCTV. It was suggested to the RIP(S)A co-ordinator that the following language or similar be included in the core 'Principles' section:

'We will only permit the use of CCTV in a pre-planned and targeted manner subject to authorisation and strict privacy safeguards under RIP(S)A.'

The Council may wish to use the specific term Directed Surveillance, although as this is to be a public-facing document, the term will need to be properly defined if it is.

5.23 In practice, the only third-party user of the public-space CCTV system is Police Scotland and the RIP(S)A requirements are set out with precision and clarity as the main schedule to an Information Sharing Agreement between Edinburgh City Council and Police Scotland. This was reflected in the excellent level of understanding demonstrated by the Community Safety Manager (Shirley McLaren) and the CCTV Operations Supervisor (Ben Quinn). I had a high degree of confidence that robust and effective systems were in place and that no unauthorised surveillance could occur.

Covert Human Intelligence Sources (CHIS)

5.24 Since the last inspection there have been no authorisations for the use and conduct of a CHIS. This reflects the widespread practice common amongst Scottish local authorities of never or rarely authorising CHIS. The possibility was discussed within the focus group and there is no bar on the use of CHIS but there are very few circumstances where it might be necessary for the Council to obtain a CHIS authorisation. One of the difficulties may be the lack of available specialist CHIS handler and controller training tailored to the requirements of local authority officers.

Direct Involvement (Self-authorisation)

5.25 There were no instances of self-authorisations. Edinburgh Council has only two AOs (not including the Chief Executive and another AO currently absent on secondment). Care must be taken to ensure that with such a small number of AOs available that no

self-authorisation occurs, although it should be noted that both AOs are of such seniority that they are significantly removed from operational planning and direction.

Communications Data (CD)

5.26 The Council retained the ability to obtain communications data under the provisions of Part 2 of RIPA during the period under inspection, however no applications were made and no communications data obtained. The Council maintains a CD policy and the RIP(S)A Co-ordinator acts as the Designated Person. Edinburgh City Council is one of the few Scottish Local Authorities inspected by IPCO that maintains a CD policy. This is good practice as although applications for CD are dealt with by the National anti-Fraud Network (NaFN), applications still need to be initiated and the subsequent product dealt with lawfully if the need should ever arise.

R. v Sutherland considerations

5.27 It was clear that authorised conduct was fully discussed with applicants following the granting of authorisations. Fuller description of the conduct authorised in the written authorisation as already recommended will further ensure that those exercising investigatory powers do not go beyond what has been authorised. It is worth emphasising to AOs, applicants and operational staff that they should always see a copy of the authorisation once granted so they are in no doubt as to what the authorisation permits. It is also good practice to make a record or note they have done so.

Policy and Procedure

5.28 The Council had a full and effective suite of RIP(S)A and CCTV related policies and operational procedures that are readily accessible by all staff. Significant changes in the law, such as the introduction of the Investigatory Powers Act 2016, should trigger review as well as other events, such as input from elected officials when they set policy, and the findings of any IPCO inspection that calls for changes in policy. The RIP(S)A Co-ordinator maintains a full record of the development of these policies, although it would be good practice if the policy was also given a clearly identifiable 'effective date' and version number. This will help ensure users are always referring to the most up-to-date policy.

5.29 **Observation 2 (O2). The Council should adopt a method of indicating effective-from and version control for its RIP(S)A related policies.**

Related Training

5.30 In the past, the Council has undertaken tiered training of staff, with specialist external training for authorising officers and other key users of RIP(S)A as well as more general RIP(S)A awareness training developed in partnership with and delivered by Queen Margaret University. Over 200 council officers attended this training. The value of this is reflected in the quality of its policy, procedures and the general level of knowledge demonstrated by operational staff during the focus-group session. This is well worth maintaining, especially as the level of practical experience declines. It would be timely for Edinburgh City Council to conduct a training needs analysis, particularly with consideration given to the challenges associated with the growth of on-line activity by the public that engages the council's statutory responsibilities in relation to anti-social behaviour, public health and social care and consider what would be appropriate training to meet these demands. As discussed in the focus group, some growing

problems may require consideration of deployment of techniques such as on-line CHIS that the Council has little or no experience of using. It will be hard for the SRO to have confidence that this can be done appropriately without the necessary investment in training. Any RIP(S)A related training received by staff should be recorded.

5.31 **Recommendation 2 (R2): It is recommended that the Council undertake a RIP(S)A training needs analysis and ensures staff receive training as identified. A central register of RIP(S)A related training should be maintained.**

5.32 One other way in which the SRO can maintain the integrity of the RIP(S)A processes when numbers of actual authorisations has declined is to undertake periodic desk-top training exercises to test different scenarios and aspects of the legislations. This could also be supplemented with a 'RIP(S)A forum' or similar, which would be a scheduled meeting which would bring applicants, AOs and operational-level staff together with the SRO/RIP(S)A co-ordinator to discuss issues such as progress on the implementation of recommendations, changes in the law, new case law, new technologies, new problems or threats which may be relevant to RIP(S)A etc. This could be held as part of the preparations for the annual report to elected members.

5.33 **Observation 3 (O3): The Council should consider running one or more RIP(S)A authorisation exercises on an annual basis as well as instituting a RIP(S)A forum.**

6 Conclusion

6.1 This was an excellent inspection. Despite the significant decline in the number of RIP(S)A authorisations, the SRO has ensured the integrity of Edinburgh's RIP(S)A processes. The Council clearly benefits from the knowledge and experience of the RIP(S)A Co-ordinator, who has been in the role since 2006. With continued investments in training I have no doubt that Edinburgh City Council will continue to achieve this high-level of compliance and should feel confident in its use of RIP(S)A authorisations when deemed necessary and proportionate.

7 List of records reviewed

7.1 For completeness, a full list of all records viewed during the inspection is captured below in Table 4.

7.2 Records listed here may have been viewed fully or only in part depending on the inspection methodology and approach taken.

Total records viewed at Inspection per power	Operation URN	Operation name
Directed Surveillance (3)	1617/001	N/A
	1617/002	N/A
	1617/004	N/A

Table 4. List of records viewed

Yours sincerely,

Brendan Hughes
IPCO Inspector

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 ('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 Head of Legal and Risk 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 Head of Legal and Risk 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

This policy shall be kept under review by the Head of Legal and Risk.

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

(iii) 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.

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

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

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 Head of Legal and Risk 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 Head of Legal and Risk 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 Head of Legal and Risk.

Appendix 4 – RIP(S)A Audit Recommendations Action Plan

RIP(S)A Audit Recommendations Action Plan

Action	Method	Estimated completion date
Recommendation 1: It is recommended that the Council fully implements the requirement to ensure that elected representatives have the opportunity to review the Council's use of RIP(S)A and set policy at least once a year.	Present annual report to Corporate Policy and Strategy Committee. Report will advise members of outcome of inspection and seek approval for revised policies including appropriate updates. Thereafter will report annually after annual return submitted to IPCO.	30 June 2019
Recommendation 2: (a) It is recommended that the Council undertakes a RIP(S)A training needs analysis and ensures staff receive training as identified. (b) A central register of RIP(S)A related training should be maintained.	(a) The Council has agreed to run a one day refresher training event for Senior Responsible Officer, RIP(S)A Coordinator , Authorising Officers and other key staff. The Council is undertaking a training needs analysis of areas which may be required to use or understand the relevant policies. The Council expects to procure a half-day refresher training event from a further or higher education provider. Procurement is underway. (b) The Council maintains and will regularly update this training record.	(a) 30 April 2019 30 June 2019 Three year provision from 1 September 2019 (b) Ongoing

Observation 1: The formal recording of legal review of RIP(S)A applications prior to authorisation is an example of good practice that introduces extra safeguards.	Checks will be maintained	Complete
Observation 2: The Council should adopt a method of indicating effective-from and version control for its RIP(S)A related policies.	Introduce version controlled policy documents, and maintain a library of previous and current versions. New versions to be approved by committee.	14 May 2019
Observation 3: (a) The Council should consider running one or more RIP(S)A authorisation exercises on an annual basis; (b) The Council should institute a RIP(S)A forum.	(a) and (b) six-monthly meetings to be introduced in Spring and Autumn each year which will undertake exercises on authorisation	(a) and (b) 30 June 2019