AGENDA ITEM No.3

EAST RENFREWSHIRE COUNCIL

CABINET

27 August 2020

Report by the Chief Officer – Legal and Procurement

REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000

PURPOSE OF REPORT

1. To provide Cabinet with the results of the Investigatory Powers Commissioner's Office (IPCO) inspection of the Council's surveillance practice undertaken in November 2019

2. To seek Cabinet approval to the amendment of the Council's Procedure on Covert Surveillance to reflect the recommendations made in the IPCO report following the inspection.

3. To report on surveillance activity undertaken by the Council during 2019/20

RECOMMENDATIONS

4. The Cabinet is asked to:-

   (a) note the terms of the IPCO inspection report attached at Appendix 1;

   (b) note the use of directed surveillance and Covert Human Intelligence Sources during the period 2019/20; and

   (c) approve the revised Procedure on Covert Surveillance attached at Appendix 2

BACKGROUND

5. The Regulation of Investigatory Powers (Scotland) Act 2000 (referred to as RIPSA) came into effect on 2 October 2000.

6. The purpose of RIPSA is to ensure that public authorities make only lawful use of covert surveillance and covert human intelligence sources (which together are referred to as covert surveillance in this Report). The Act regulates these activities by requiring that surveillance operations be justified and authorised by a senior officer of the Authority.

7. The Investigatory Powers Commissioner's Office oversees the regulatory framework. The Commissioner carries out regular inspections (every 3 years) of all public bodies who carry out covert surveillance in terms of the Act and make various recommendations in relation to the procedures adopted by these bodies. East Renfrewshire Council's most recent inspection took place between October and December 2019.

INSPECTION FINDINGS

8. The inspection was undertaken by way of a desktop exercise and involved examination of all the Council's policies, procedures and practice in respect of surveillance operations as well as an assessment of all surveillance authorisations applied for during the 3 year period leading up to the inspection date.

9. The Inspector's findings are set out in his inspection report dated 16 December 2019 which is attached as Appendix 1. Generally, the report is positive. It confirms the lawfulness of the Council's current surveillance practice and endorses its use as relevant and proportionate to the issues it seeks to address. It also confirms that all recommendations from the previous inspection in 2016 have been given effect. The report makes two specific recommendations as to future practice. These relate respectively to the need for applicants to thoroughly address necessity, proportionality and collateral intrusion for each subject for whom surveillance is sought within an overarching application and the management of evidence obtained during surveillance activities. A number of observations in praise of good practice are also made.

CHANGES TO COUNCIL PROCEDURE

10. The IPCO inspection report makes two recommendations and a number of observations regarding future authorisations. In order to ensure that these comments are given effect and are reflected in day to day practice the Council's procedures on Covert Surveillance have been updated. The proposed revised version is attached as Appendix 2. As recommended, reference to relevant sections of the Scottish Government Codes of Practice have been inserted and the participation of the Chief Officer- Legal and Procurement as Senior Responsible Officer limited in respect of particular applications.

11. Further detail has also been added to the sections on necessity, proportionality and collateral intrusion providing further instruction to both applicants and authorising officers as to what is required of them in making and assessing applications. Authorising officers are also reminded of the need to give directions as to the use, storage and ultimate destruction of any evidence obtained through authorised surveillance operations.

USE OF RIPSA DURING 2109/20

12. During the period 1 April 2019 to 31 March 2020 the Council authorised directed surveillance of 14 separate individuals under 3 overarching authorisations. Two were for online investigations into sale of illicit goods, whether counterfeit or stolen and were undertaken by officers of Trading Standards Scotland. The other related to an application by officers of the Education service to investigate suspected fraudulent misrepresentation to gain entry to a local school. No use was made of Covert Human Intelligence Sources.

13. It was originally intended to present this report to Cabinet in May 2020 with annual reports being submitted at the same time in each subsequent year. Due to the implications of the Covid-19 lockdown, this year's report has been necessarily delayed. In the interim period since 31 March, a further authorisation for directed surveillance has been granted covering 1 individual. This related to a local trading standards operation.

FINANCIAL IMPLICATIONS

14. There are no direct financial implications arising from this report.

RECOMMENDATIONS

15. The Cabinet is asked to:-

(a) note the terms of the IPCO inspection report attached at Appendix 1;

(b) note the use of directed surveillance and Covert Human Intelligence Sources during the period 2019/20; and

(c) approve the revised Procedure on Covert Surveillance attached at Appendix 2

Author: Mr Gerry Mahon, Chief Officer – Legal and Procurement:
Tel No: 0141 577 3801
e-mail: gerry.mahon@eastrenfrewshire.gov.uk

Desktop Inspection Report
East Renfrewshire Council

Contents

1 Introduction

1.1 This desktop inspection has been conducted to assess East Renfrewshire Council's level of compliance with the Regulation of Investigatory Powers (Scotland) Act (RIPSA) 2000 and all associated codes of practice in respect of its use of directed surveillance and covert human intelligence sources (CHIS).

1.2 The inspection was conducted by IPCO Inspector Paul Donaldson.

1.3 East Renfrewshire Council employs around 3,500 staff to deliver the full spectrum of services ranging from Education, and Environmental Services, through to Social Care, Housing, Transport and Licensing.

1.4 The Chief Officer, Legal and Procurement, Mr Gerry Mahon is nominated as the Senior Responsible Officer (SRO) in relation to RIPSA. Gerry.Mahon@eastrenfrewshire.gov.uk

1.5 The Chief Executive is Ms Lorraine McMillan –

Lorraine.McMillan@eastrenfrewshire.gov.uk

2 Inspection methodology

2.1 The inspection comprised a desktop review of policy documents, training records, and the examination of applications and authorisations completed since the last inspection in December 2016.

2.2 The necessary completed questionnaire and associated documents were provided by Mr Gerry Mahon which enabled a desktop assessment of compliance to be conducted.

2.2 Statistics relating to previous authorisations and those examined is captured below and a full list of references is included at Annex A.

	December 2016 – December 2019	
East Renfrewshire Council	**Total authorisations in current inspection period**	**Total records viewed at Inspection**
Directed Surveillance	4	4
CHIS	0	N/A

Table 1. Key Statistics

3 Key findings

3.1 Recommendations

3.1.1 The inspection found that East Renfrewshire Council maintains a good overall standard of compliance with the legislation and relevant codes of practice, although two formal recommendations are required. The two recommendations made in the previous

inspection have been addressed and can be discharged (see below). To assist in maintaining the current good standards, some observations are offered, alongside identified areas of good practice.

3.1.2 The two recommendations being made are listed in table 2 below:

Number	Reference	In relation to	Recommendation	Recommendation type
1	**5.4.5**	**Directed Surveillance**	Applicants to ensure that for all proposed subjects and tactics sought, the key elements of necessity, proportionality and collateral intrusion are addressed for each.	Core recommendation - improvements must be made
2	**5.4.12**	**Management of product**	Authorising Officers should provide direction in relation to the management of product/material upon the cancellation of directed surveillance authorisations	Core recommendation - improvements must be made

Table 2: recommendations

3.2 Observations

3.2.1 The key observations arising from the inspection are listed in table 3 below:

Number	Reference	In relation to	Observation	Observation type
O1	**5.3.2**	**RIPSA Policy**	RIPSA Policy being published online	Observation – praise of good practice
O2	**5.3.4**	**Authorisation procedure**	SRO to limit his involvement in the RIPSA process to those oversight responsibilities outlined in the codes of practice	Observation – comment
O3	**5.3.5**	**Governance**	Maintenance of a register of issues to identify training needs	Observation – praise of good practice
O4	**5.3.7**	**Training**	The use of webinars and online training to maintain the knowledge and skillset of staff	Observation – praise of good practice
O5	**5.3.9**	**RIPSA**	Reporting to Elected Members to take place at least once per year as per the codes of practice.	Observation - comment
O6	**5.4.7**	**RIPSA**	Applicants should provide more detail in reviews and renewals of the frequency, nature and value of surveillance	Observation - comment

			deployments and the product obtained.	
O7	**5.4.10**	**RIPSA**	Authorising Officers should describe in detail the activity they are specifically authorising to comply with paragraph 4.8 of the code of practice[1]	Observation - comment

Table 3. Key observations resulting from inspection

4 Previous recommendations

4.1 The previous inspection made two recommendations and the following progress was noted:

R1 *- The Council should conduct an assessment across all departments to determine its current and future requirements to use the Internet for investigative and research purposes. Once complete, the Council should determine what further training and guidance is required to ensure staff undertaking such activity do so in accordance with its surveillance policy (paragraphs 6.4 to 6.6).*

Discharged. A survey was conducted in early 2017 and reported on to the Council's Corporate Management Team (CMT) in June 2017 which included a draft guidance document for issue to staff via the Council's intranet. After agreement by the CMT the guidance was issued. The guidance was subsequently revised and reissued in 2018 to take account of the increased content on the topic set out in the revised Scottish Government Code of Practice for Covert Surveillance (December 2017). Apart from appropriately trained staff from Trading Standards Scotland (TSS) the survey concluded that very little use was being made of internet research as an investigative tool.

R2 *– The Council must ensure that when granting an authorisation for CHIS, the Authorising Officer has confirmed that arrangements are in place for the management and oversight of the use made of that CHIS as required by Section 7(6)(a) and (b) of RIP(S)A, and paragraphs 6.5 to 6.9 of the Code of Practice. It is best practice that the names of the individuals charged with these responsibilities are included on the authorisation. The Authorising Officer must also ensure an appropriate risk assessment, as required by paragraph 6.13 of the Code of Practice, has been completed (see paragraphs 8.14 to 8.16).*

Discharged. Despite there being no further use made of CHIS in support of investigations, appropriate steps were taken to reinforce these requirements in both the Council's procedures and application forms for CHIS authorisation, review and renewal. These forms duly require the handler and controller to be named, as per Section 7 (6) (a) and (b) of RIPSA and for the Authorising Officer to acknowledge same in their authorisation considerations. In relation to the second part of this recommendation outlining the need for risk assessments, the Council policy document

[1] Scottish Government Code of Practice, Covert Surveillance and Property Interference, December 2017

at paragraph 9.2.9 highlights the requirements set out in the Code of Practice at paragraph 6.13[2].

5 Inspection findings

5.1 Errors

5.1.1 No errors have been reported to IPCO and none were identified in the applications and authorisations examined.

5.2 Confidential Information

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

5.3 Policy and Procedures

5.3.1 The Council maintains a comprehensive policy document which provides clear and accurate guidance covering the use of RIPSA and is published on the Council's website. The policy contains pro-forma examples of the forms used for the Council's use of its relevant powers and directions to practitioners on how to complete an application. The policy also directs readers to the primary legislation although it would benefit practitioners to be signposted also to the relevant codes of practice.

5.3.2 Publication of relevant RIPSA guidance on the internet/intranet is viewed as good practice.

5.3.3 Paragraph 9.1.1 of the policy describes a pre-application process which involves an assessment being made by the SRO of the appropriateness of any proposed application. Any considerations to be made around applications for directed surveillance or CHIS are the preserve of the Authorising Officer and prescribed in the legislation. The SRO has other responsibilities described in paragraphs 9.1[3] and 4.41[4] and any involvement should be limited to those, in order to maintain the integrity of the process.

5.3.4 SRO to limit his involvement in the RIPSA process to those oversight responsibilities outlined in the codes of practice.

5.3.5 Applications and subsequent authorisations are completed in paper copy and the details for every application are recorded on a central record of authorisation maintained by the SRO. The process identified as being good practice at the last inspection, involving the maintenance of a register of issues, continues and enables any learning and development needs to be identified quickly and addressed through additional guidance or further training when necessary.

5.3.6 The investment in regular and relevant training delivered externally (by Police Scotland) and internally ensures practitioners are suitably qualified to perform their respective roles. This has included very useful refresher training provided through the

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

medium of webinars created by a reputable national legal firm which allows Authorising Officers and applicants to maintain currency in the disciplines associated to RIPSA. These webinars are comprehensive in structure, containing very good content and are identified as being evidence of good practice in relation to addressing any training needs.

5.3.7 The use of webinars and online training to maintain the knowledge and skillset of staff.

5.3.8 The Council has a process where detail around its use of RIPSA is reported to the East Renfrewshire Council Cabinet which comprises Elected Members. It was noted that the most recent report dated 10 October 2019 outlined the use of the powers for the period between 2017 and 2019. It should be noted that this reporting process should occur at least once a year as outlined in paragraph 4.43[5].

5.3.9 Reporting to Elected Members to take place at least once per year as per the codes of practice.

5.4 Directed Surveillance

5.4.1 All applications and authorisations for directed surveillance completed since the last inspection were examined and found to have been completed to a good standard. All applications for directed surveillance related to the initial stages of online investigations into the supply of counterfeit goods and consumer protection issues being facilitated through online marketplaces.

5.4.2 The Council has adopted a process of applying for and authorising 'overarching' directed surveillance authorisations based on specific categories crime types, all being conducted online, which impact on the Council and are subject to proactive investigations by TSS. It is appropriate that applications are constructed around crime types, appropriately categorised based on current intelligence, similar *modus operandi* and criminal intent, to avoid authorisations being granted which may fall to be excessively wide in scope amounting to 'fishing expeditions'.

5.4.3 The initial activity sought will be for the deployment of online investigative resources to engage with already identified social media accounts for the purpose of identifying the account holder and arranging the test purchase of relevant goods, without venturing towards the need for CHIS authorisations. Operational objectives are described well, and no long-term engagement is planned, with no intention of establishing and maintaining relationships that would necessitate the authorisation of CHIS.

5.4.4 The applications and authorisations examined could be described as 'overarching' in nature, with specific individuals/accounts being added or removed by way of review during the life of the authorisation. Most individuals/accounts sought to be added were accompanied by succinct and relevant intelligence cases describing the necessity for the tactic, although applicants should be reminded that each individual/account or

[5] Scottish Government Code of Practice, Covert Surveillance and Property Interference, December 2017

tactic should be subject to specific considerations in terms of proportionality and collateral intrusion (paragraphs 4.5, 4.7, 4.11 and 4.12[6]). It is not enough to batch unconnected individuals without providing bespoke considerations and it is important to do so to allow the Authorising Officer to make distinctions, when necessary, to avoid the blanket authorisation of upwards of 18 unconnected individuals (URN 209) without specific considerations being attached.

5.4.5 Applicants to ensure that for all proposed subjects and tactics sought, the key elements of necessity, proportionality and collateral intrusion are addressed for each.

5.4.6 The four applications and authorisations were all overarching in nature and subject to several reviews and renewals where subjects, or additional tactics (physical surveillance to monitor test purchases) are either added, removed or continued by the Authorising Officer dependent on the progress of operations. At times, due to the number of subjects being authorised, mostly within separate TSS investigations, following the progress of how the authorised activity was benefiting the inquiry was somewhat difficult. This was exacerbated by the fact that applicants, whilst providing a relevant summary of progress, did not consistently detail in reviews or renewals any specifics around the frequency, nature or product obtained through surveillance deployments, or an assessment as to any benefit being derived from the covert activity.

5.4.7 Applicants should provide more detail in reviews and renewals of the frequency, nature and value of surveillance deployments and the product obtained.

5.4.8 The process of reviewing and renewing the authorisation should ensure that the Authorising Officer has enough detail to allow appropriate considerations to be made in line with paragraphs 4.36, 4.37, 4.39 and 5.16[7]. It is also important to provide the Authorising Officer some assurance and comfort that the activity being conducted is not going beyond what is authorised, especially in the arena of online directed surveillance and the attendant risk attached where excessive communication with subjects may follow, which may necessitate a CHIS authorisation.

5.4.9 Authorising Officers, upon being presented with applications, apply their considerations to the relevant forms, and in most cases provide adequate considerations outlining their satisfaction that the conduct sought is necessary and proportionate. In general terms the activity being authorised by them could be described in greater clarity to ensure operatives, in line with paragraph 4.8 of the Code of Practice[8], can comply with their *R v SUTHERLAND* responsibilities.

5.4.10 Authorising Officers should describe in detail the activity they are specifically authorising to comply with paragraph 4.8 of the Code of Practice[9].

[6] Scottish Government Code of Practice, Covert Surveillance and Property Interference, December 2017
[7] Ibid
[8] Scottish Government Code of Practice, Covert Surveillance and Property Interference, December 2017
[9] Ibid

5.4.11 Cancellations were submitted timeously although applicants should provide more detail around the benefits brought to an investigation through the deployment of covert tactics; but more importantly, the type and extent of the product and material obtained by it and how it is to be managed in accordance with the provisions contained within Chapter 8[10]. Authorising Officers provide little commentary upon cancellation forms and should ensure they articulate some direction or instruction for the management of product, as per good practice described in Chapter 8 of the Code of Practice[11].

5.4.12 Authorising Officers should provide direction in relation to the management of product/material upon the cancellation of directed surveillance authorisations.

5.4.13 Covert surveillance, particularly online directed surveillance, is being used to good effect by East Renfrewshire Council to tackle some of its enforcement priorities. The use of the 'overarching' authorisations has been found to be overall fully compliant, but if not managed appropriately, carries with it a significant risk of generating relevant errors. This risk could be very much reduced by ensuring that the nature, frequency and conduct of deployments are better described in reviews, renewals and cancellations. Attention is required to ensure that the product and material obtained is detailed within the relevant paperwork, which will allow the Authorising Officer to assess the nature of the material and be assured that operatives do not extend their conduct beyond what is authorised.

5.4.14 The use of the 'overarching' authorisation, managed robustly, can be regarded as good practice given it significantly reduces the bureaucracy attached to the RIPSA process within a very proactive local authority. Managed appropriately, it allows the Authorising Officer to have a comprehensive overview of the activity being undertaken and how its use is benefiting East Renfrewshire Council investigations, without requiring the management of multiple separate authorisations.

5.5 Covert Human Intelligence Sources (CHIS)

5.5.1 The Council has not made any use of CHIS in this inspection period although it is not ruled out as a tactic to be considered in the future. The policies and procedures, along with the knowledge and experience of staff, some from a previous covert policing background, give some confidence that any future use would be compliant, although some further training may benefit those designated to be involved in any CHIS handling. East Renfrewshire Council has recruited individuals with covert policing experience and enjoys strong links with Police Scotland and would be confident in seeking its assistance in such matters if required.

5.5.2 Given the extensive use being made of the internet for investigative purposes, the potential for the use of TSS online investigators as CHIS conducting low level undercover work 'on-line' is a distinct possibility. If the authority is to embark on this activity as an investigative tool, it is suggested it engages with law enforcement partners to ensure the skillset of staff is appropriate to ensure welfare and security

[10] Ibid
[11] Ibid

considerations are fully catered for in terms of the responsibilities laid down in section 7(6) (a) and (b) of RIPSA.

6 Conclusion

6.1 This inspection has established that East Renfrewshire Council has generally maintained a professional, legally compliant, and operationally efficient approach to the use of covert investigation powers. Its use of available powers is only embarked upon where the opportunity to deploy overt solutions have been exhausted, and it is significant that most of this activity is conducted online where no other investigative option is available.

6.2 The use of 'overarching' directed surveillance authorisations is rather innovative although, whilst the process reduces the bureaucratic burden on applicants and Authorising Officers, to ensure continuing compliance it requires close and robust scrutiny by Authorising Officers, taking into consideration the recommendations and observations made in this report.

6.3 The Inspector would like to extend thanks to Mr Gerry Mahon for providing the comprehensive suite of documents to enable a thorough inspection.

Paul Donaldson

Paul Donaldson
Inspector IPCO

Annex A

For completeness, a full list of all records viewed during the inspection is captured below. All records were reviewed in full.

Directed Surveillance URN	**Operation name**
URN 209	JASPER
URN 209 (2)	JASPER
	DRAM
URN 210	JASPER

Appendix 2

REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000

PROCEDURE ON COVERT SURVEILLANCE

Version 7
July 2020

EAST RENFREWSHIRE COUNCIL

REGULATION OF INVESTIGATORY POWERS (SCOTLAND) ACT 2000

PROCEDURE ON COVERT SURVEILLANCE

1. INTRODUCTION

1.1 In some circumstances, it may be necessary for council employees, in the course of their duties, to make observations of a person or persons in a covert manner (i.e. without that person's knowledge), or to instruct third parties to do so on the Council's behalf. By their nature, actions of this sort are potentially intrusive (in the ordinary sense of the word) and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights and the Human Rights Act 1998 ('the right to respect for private and family life').

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

1.3 The Chief Officer (Legal & Procurement) has overall responsibility within East Renfrewshire Council for monitoring compliance with the provisions of the Regulation of Investigatory Powers (Scotland) Act 2000 and acts as Senior Responsible Officer under the legislation. He shall keep and maintain the Central Register.

2. OBJECTIVE

2.1 The objective of this procedure is to ensure that all covert surveillance by council employees is carried out effectively, while remaining in accordance with other Council procedures and the law. This procedure should be read in conjunction with the relevant legislation, the Scottish Government's Codes of Practice on Covert Surveillance and Property Interference https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice/pages/1/

and Covert Human Intelligence Sources

https://www.gov.scot/publications/covert-human-intelligence-sources-code-practice/

('the Codes of Practice') and any guidance which the Investigatory Powers Commissioner's Office (IPCO) may issue from time to time.

2.2 If the procedures outlined in this document are not followed, any evidence acquired may not have been acquired lawfully. Such evidence may not be admissible in court, and in respect of criminal proceedings, the Procurator Fiscal may decide not to prosecute on the basis of evidence unlawfully obtained. Also, the Council may be exposed to legal challenge.

2.3 These procedures reference and link to relevant parts of the Covert Surveillance and Property Interference Code of Practice 2017 as further guidance. Both applicant and authorising officers are encouraged to access this material to maintain a thorough knowledge of best practice in relation to directed surveillance and the use of Covert Human Intelligence Sources.

3. PUBLICITY

3.1 Copies of this Policy and of the Codes of Practice are available for inspection by any person at the Council Headquarters, Eastwood Park, Giffnock and on the Council's web site.

4. COMPLAINTS TO THE INVESTIGATORY POWERS TRIBUNAL

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

Investigatory Powers Tribunal,
PO Box 33220,
LONDON
SW1H 9ZQ

5. SCOPE OF THE PROCEDURE

5.1 Subject to the exceptions identified in paragraph 5.2 below, this procedure applies in all cases where directed surveillance or the use of a covert human intelligence source is being planned or carried out.

(a) Directed surveillance is defined as "covert surveillance that is not intrusive but is carried out in relation to a specific investigation or operation in such a manner as is likely to result in the obtaining of private

information about any person" [Scottish Government Code of Practice on Covert Surveillance and Property Interference 2017, para 2.4]

(b) A Covert Human Intelligence Source (CHIS) is defined as a person who establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating anything that:

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

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

5.2 This procedure does not apply to:-

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

- ad-hoc covert observations that do not involve the systematic surveillance of specific person(s).

- observations that are not carried out covertly, or unplanned observations made as an immediate response to events.

- 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.

5.3 In cases of doubt as to whether the procedure is applicable, the authorisation procedures described below should however be followed.

6. PRINCIPLES OF SURVEILLANCE

6.1 In applying for and granting authorisations for covert surveillance, and in planning and carrying out such surveillance, East Renfrewshire Council employees shall at all times comply with the following principles:

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

- Lawful purposes - covert surveillance shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in RIPSA), i.e. it must be:

    - for the purpose of preventing or detecting crime or the prevention of disorder; and/or

    - in the interests of public safety; and/or

    - for the purpose of protecting public health.

- Necessity - covert surveillance shall only be undertaken where there is no reasonable and effective alternative way of achieving the desired objective(s). The surveillance must be necessary for one of the purposes set out above. In order to establish the necessity of any surveillance, the conduct which the surveillance is intended to detect or prevent must be clearly identified. Both the need for surveillance and the particular techniques to be used in that surveillance must be justified

- Proportionality – the use and extent of covert surveillance shall not be excessive i.e. it shall be in proportion to the significance of the matter being investigated. Before deciding to carry out covert surveillance, proper consideration shall be given to the nature of the matter being investigated and whether it is sufficiently serious to warrant the use of covert surveillance and the particular type of covert surveillance being proposed. Consideration must also be given to the extent to which the surveillance will unnecessarily intrude on the privacy of the target of the surveillance and any others. Before deciding to carry out covert surveillance full and proper consideration will be given to any alternative methods of obtaining the information. Covert surveillance will only be authorised if these alternative methods have been discounted for good reason and the surveillance is the only reasonable way of obtaining the necessary result.

  In addressing proportionality officers should:-

    - Balance the size and scope of the operation against the seriousness and extent of the conduct the surveillance is intended to address

    - Ensure surveillance techniques employed will cause the least possible intrusion on the target of the surveillance and others

    - Ensure that the surveillance is, after consideration of alternatives, the only reasonable way of obtaining the necessary result

    - Describe other discounted methods of obtaining information and narrate the basis on which they were discounted

- Damage - Employees carrying out covert surveillance shall not cause damage to any property or harass any person.

- Intrusive surveillance - no activity shall be undertaken that comes within the definition of 'Intrusive Surveillance', i.e. if it involves surveillance of anything taking place on residential premises or in a private vehicle, and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device.

- Collateral intrusion - reasonable steps shall be taken to minimise the acquisition of information that is not directly necessary for the purposes of the investigation or operation being carried out.

  Authorisation - all directed surveillance or the use of a covert human intelligence source shall be authorised in accordance with the procedures described below.

6.2 When an overarching authorisation is sought in respect of a number of different individuals the key elements of necessity, proportionality and collateral intrusion must be addressed for each one in the application.

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

Further guidance: Part 4 of the Covert Surveillance and Property Interference Code of Practice 2017
https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice/pages/4/

7. SEEKING AUTHORISATION

7.1 When is Authorisation Required?

7.1.1 Authorisation is required for directed surveillance or the use of a covert human intelligence source, where any such operation is planned, is likely to record "private information" about a person or persons, and is conducted in such a manner that the person or persons subject to the surveillance are unaware that it is or may be taking place. Authorisation is required where the activity is carried out by council officers themselves or by third parties carrying out surveillance on behalf of or under the instructions of the Council.

7.2 Who May Seek Authorisation?

7.2.1 Any officer whose duties involve activity falling within the above description may seek authorisation to do so and must seek authorisation prior to carrying out any surveillance described in the paragraph headed “Scope of Procedure”.

7.3 Who May Authorise?

7.3.1 Applications for directed surveillance or the use of a covert human intelligence source shall be authorised by any one of the following officers:-

Lorraine McMillan, Chief Executive,
Caroline Innes, Deputy Chief Executive,
Joe Abrami, Principal Solicitor, Chief Executive’s Office
Julie Murray, Director of East Renfrewshire Health and Social Care Partnership
Jamie Reid, Data and Information Manager, Corporate and Community Services

7.3.2 The authorising officer should not be directly involved in the investigation to which the surveillance relates. In this regard, it is expected that Applicants will typically apply to authorising officers from outwith their own service unless it is unreasonable or impractical in the circumstances to do so.

7.3.3 Where there is a significant risk of acquiring confidential material, an application shall require to be authorised by the Chief Executive or, in her absence, the Deputy Chief Executive.

7.3.4 When the use of a juvenile or vulnerable covert human intelligence source is sought, an application shall always require to be authorised by the Chief Executive or, in her absence, the Deputy Chief Executive**.**

8. CONFIDENTIAL MATERIAL

8.1 The Codes of Practice give the following advice in relation to what constitutes confidential material:

a. Communications subject to Legal Privilege

In Scotland, the law relating to legal privilege rests on common law principles. In general communications between professional legal advisers and their clients will be subject to legal privilege unless they are intended for the purpose of furthering a criminal act or to obtain advice thereon.

Legal privilege does not apply to communications made with the intention of furthering a criminal purpose (whether the lawyer is acting unwittingly or culpably). Legally privileged communications lose their protection if, for example, the professional legal adviser is intending to hold or use them for a criminal purpose. But privilege is not lost if a professional legal adviser is properly advising a person who is suspected of having committed a criminal offence. The

concept of legal privilege applies to the provision of professional legal advice by any individual, agency or organisation qualified to do so.

b. Communications involving confidential personal information

Confidential personal information is information held in confidence relating to the physical or mental health of a person or spiritual counselling of such a person e.g. between a priest and parishioner. Such information, which can include both oral and written communications, is held in confidence if it is held subject to an express or implied undertaking to hold it in confidence or it is subject to a restriction on disclosure or an obligation of confidentiality contained in existing legislation. Examples include consultations between a health professional and a patient or information from a patient's medical records.

c. Communications involving confidential journalistic material

Confidential journalistic material includes material acquired or created for the purposes of journalism and held subject to an undertaking to hold it in confidence, as well as communications resulting in information being acquired for the purposes of journalism and held subject to such an undertaking. Journalists have a restricted right not to disclose as source of information which is regulated by section 10 of the Contempt of Court Act 1981.

d. Communications involving confidential constituent information

Confidential constituent information includes material passed confidentially between a MP or MSP and their constituent in respect of constituency matters.

Further guidance: Part 8, paragraphs 8.22 onwards of the Covert Surveillance and Property Interference Code of Practice 2017
https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice/pages/8/

9. THE AUTHORISATION PROCESS

9.1 Directed Surveillance

Pre- application

9.1.1 Prior to seeking authorisation, the Applicant should advise the Chief Officer – Legal and Procurement (by secure e-mail) of the proposed application. The Chief Officer–Legal and Procurement will issue a Unique Reference Number (URN) to the Applicant. This number should thereafter be inserted on the front page of all documents relating to the application.

Initial authorisation

9.1.2 Once the URN is issued, the Applicant should submit the application using Form 1 (as referred to in the Documents section of this procedure) to an appropriate authorising officer. If he or she is satisfied that the application meets the criteria outlined in Paragraph 6 above the application may be authorised.

9.1.3 The authorising officer should state explicitly in his/her own words what is being authorised (which may not be the same as that sought by the applicant) and should describe it in detail. They should record who is the subject of the surveillance, what is authorised to be done, where the surveillance can be done and during what times, the manner in which the surveillance is to be undertaken and why it is both proportionate and necessary. The person carrying out the surveillance must have a clear indication of the extent and limits of the authorisation.

9.1.4 Any difference between the authorisation and the terms of the application should be noted and explained by the authorising officer.

9.1.5 The authorising officer should sign and date the authorisation and provide a copy to the Applicant. The Authorising officer should immediately send the principal authorisation to the Chief Officer – Legal and Procurement.

9.1.6 Authorisations for directed surveillance will lapse after the expiry of three months. For practical purposes, the relevant period ends as at 2359 hours on the day preceding.

Renewal

9.1.7 If the applicant considers that surveillance remains necessary and proportionate but the expiry of the initial authorisation is imminent, they may seek renewal of the authorisation.

9.1.8 In any application for renewal, the applicant should include detail of the frequency, nature and value of surveillance undertaken to date and any evidence obtained.

9.1.9 Form 3 (as referred to in the Documents section of this procedure) should be submitted to an authorising officer in sufficient time for it to be considered prior to the expiry of the original authorisation. Renewals must be granted prior to the expiry of an existing authorisation. Renewal will be for a further period of 3 months effective from the expiry of the original authorisation.

9.1.10 The authorising officer should sign and date the renewal and provide a copy to the applicant. The principal copy should be sent immediately to the Chief Officer- Legal and Procurement.

Review

9.1.11 Authorising Officers should keep all authorisations under review and, where appropriate, cancel immediately the need for surveillance ceases. The results of all such reviews should be recorded on the appropriate review form (Form 2) , notified to the Chief Officer - Legal & Procurement and recorded in the central record of authorisations. Review dates should be directed based on the level of intrusion, collateral intrusion or likelihood of obtaining confidential material.

9.1.12 In any review, the applicant should include detail of the frequency, nature and value of surveillance undertaken to date and any evidence obtained.

Cancellation

9.1.13 Authorising officers should cancel authorisations as soon as the surveillance ceases to be necessary or proportionate. Applicants should submit Form 4 to the authorising officer for consideration when they believe such circumstances exist. An authorising officer may equally cancel an authorisation if they are in receipt of information from another source which causes them to believe that the surveillance is no longer necessary or proportionate.

9.1.14 When cancelling the authorisation the authorising officer should record the time the authorisation was cancelled and advise the applicant immediately of this fact. The reason for cancellation and the detail of the surveillance undertaken under the authorisation should be recorded. The cancellation should also include detail of the product obtained and the worth of the surveillance in the context of the investigation.

9.1.15 If relevant, the authorising officer should ensure that all surveillance equipment has been removed and should provide directions to the applicant as to how the information produced from the surveillance is to be handled.

9.1.16 The authorising officer should record whether the objectives set out in the authorisation have been met

9.1.17 Upon completion, the cancellation form should be sent to the Chief Officer – Legal and Procurement.

Further guidance: Part 5 of the Covert Surveillance and Property Interference Code of Practice 2017

https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice/pages/5/

9.2 Covert Human Intelligence Source (CHIS)

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

9.2.2 Authorisations for juvenile covert human intelligence sources will lapse after the expiry of one month. In all other cases, the authorisation for a CHIS will lapse after twelve months. For practical purposes, the relevant period ends as at 2359 hours on the day preceding.

9.2.3 Applications for authorisation for, and reviews, renewals and cancellations of, CHIS should be made and progressed using Forms referred to in the Documents section of this procedure numbered 6,7,8 and 9 respectively. The process followed shall, subject to the additional matters below, follow that as for directed surveillance.

What Additional Safeguards are Necessary before using a Covert Human Intelligence Source?

9.2.4 Prior to making an application for use of a CHIS, the Applicant should contact the Chief Officer – Legal and Procurement to discuss the appropriateness of this approach in the particular circumstances. If agreed as a suitable approach, a draft of the application should be submitted to the Chief Officer –Legal and Procurement. If the detail of the application is considered sufficient, the applicant will be provided with a URN.

9.2.5 The Applicant should submit the application to the appropriate authorising officer. When the use of a juvenile or vulnerable covert human intelligence source is sought, an application shall always require to be authorised by the Chief Executive or, in her absence, the Deputy Chief Executive.

Management of a CHIS

9.2.6 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.

9.2.7 An individual officer (known as the “”handler”) must be appointed to be responsible for the day to day contact between the source and the authority, including:

- Dealing with the source on behalf of the authority
- Directing the day to day activities of the source

- Recording the information supplied by the source

- Monitoring the source's security and welfare

9.2.8 In addition the Authorising Officer must satisfy themself that an officer (known as the "controller") has been designated responsibility for the general oversight of the use made of the source. The names of both the handler and controller should be specified in the authorisation.

9.2.9 The Authorising Officer must also ensure that a risk assessment has been carried out to determine the risk to the source of any tasking and the likely consequences if the role of the source becomes known. Such a risk assessment is required irrespective of whether the CHIS is acting in a conventional manner or in an online capacity. It will be the responsibility of the handler 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.

9.2.10 Records must also be maintained, in accordance with the relevant statutory instruments, detailing the use made of the source. It will be the responsibility of the person in day to day control of the activities of the source to maintain the relevant records. The following matters must be included in the records relating to each source:

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

Note: All officers shall conduct themselves in accordance with the requirements of the Code of Practice on Covert Human Intelligence Sources.

Use of Vulnerable Individuals as a Covert Human Intelligence Source

9.2.11 A vulnerable individual is a person who is or may be in need of community care services by reason of mental or other disability, age or illness or who is otherwise unable to take care of themselves or unable to protect themselves from significant harm or exploitation. Such individuals should not be used as a Covert Human Intelligence Source, other than in the most exceptional circumstances.

Use of a Juvenile as a Covert Human Intelligence Source

9.2.12 Special safeguards apply to the use of persons under the age of 18 as a Covert Human Intelligence Source. Children under the age of 16 must never be used to provide information against their parents or any person who has parental responsibility for them. In other cases, authorisations should not be granted unless the special provisions contained within the Regulation of Investigatory Powers (Juveniles) (Scotland) Order 2002 are satisfied. If there is any proposal to use a juvenile as a Covert Human Intelligence Source, advice must be sought from the Chief Officer – Legal and Procurement

Further guidance: Covert Human Intelligence Sources:Code of Practice https://www.gov.scot/publications/covert-human-intelligence-sources-code-practice/

9.3 Urgent applications

9.3.1 In urgent cases, an oral authorisation may be given. Urgent cases are those in which surveillance is undertaken in circumstances where it would not be reasonably practicable to obtain authorisation prior to the surveillance being carried out. This does not include surveillance as an immediate response to events (which does not fall within the scope of the Act and is not subject to the terms of this procedure).

9.3.2 Such authorisation may be given by any of the designated authorising officers. Both the person seeking the authorisation and the authorising officer must document an Oral Authorisation as soon as possible. An oral authorisation will expire after 72 hours in any case.

9.3.3 A case will not be considered urgent unless the time that would elapse before the authorising officer was available to grant the authorisation would, in the judgement of the person giving the authorisation, be likely to endanger life or jeopardise the investigation or operation. An authorisation will not be considered urgent because the need for the authorisation has been neglected.

9.3.4 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 Executive's guidance on authorising grades.

Further guidance: Part 5, paras 5.8-5.10 of the Covert Surveillance and Property Interference Code of Practice 2017
https://www.gov.scot/publications/covert-surveillance-property-interference code-practice/pages/5/

10. RISK ASSESSMENT

10.1 Before authorising any form of covert surveillance, the authorising officer should also consider whether the proposed action will place any employee or other person at risk. If so, the authorising officer shall have regard to other council procedures already in place, and should also carry out a risk assessment of the proposed course of action before authorisation is granted. Regard must be had to the specific requirements in relation to vulnerable individuals and juveniles.

10.2 The risk assessment should take into account the impact on the employee or other person if their role in the process becomes known.

11. RETENTION AND DESTRUCTION OF SURVEILLANCE EVIDENCE

11.1 Where the product of surveillance could be relevant to pending or future criminal or civil proceedings, it should be retained for a suitable further period and its retention reviewed at a future date.

Further guidance: Part 8, paras 8.17-8.21 of the Covert Surveillance and Property Interference Code of Practice 2017
https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice/pages/8/

12. INTERNET INVESTIGATIONS

12.1 A single viewing of an individual's open source social media page (such as Facebook etc.) is not automatically considered directed surveillance and as such does not generally require to be authorised provided the viewing is merely a preliminary examination of the site to establish whether it is of interest or not. If the single viewing forms part of a more extensive collection of information about the individual then a directed surveillance authorisation should be sought. Likewise, repeated viewings of the page or a systematic regime of viewing is directed and will require to be authorised as such. This is the case even though the individual has not applied privacy settings to the account which would otherwise block access. A CHIS authorisation is not generally required for such access. It will however be required in situations where a covert relationship is

likely to be formed between the applicant officer and the individual (i.e. if the surveillance activity is more than mere reading of the site's content). In such a case, a risk assessment is required (see paragraph 9.2.9 above).

12.2 The use of a disguised purchaser to conclude an electronic purchase on platforms such as E-Bay/Gumtree etc. does not generally require a CHIS provided the purchase is a simple overt process. If however the applicant requires to establish a relationship with the seller in order to prompt the sale or generate a degree of trust a CHIS authorisation will be required.

12.3 Consideration should be given to the following factors in reaching a conclusion as to whether a directed surveillance authorisation is required. If the answer to any of the questions is yes it is likely that you will need to seek authorisation.

- Is the investigation or research directed towards an individual or group of people;
- Is it likely to result in obtaining private information about a person or group of people (taking account of the guidance at paragraph 3.14);
- Is it likely to involve visiting internet sites to build up an intelligence picture or profile;
- Will the information obtained will be recorded and stored;
- Will the information be likely to provide an observer with a pattern of lifestyle;
- Will the information be combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Is the investigation or research part of an ongoing piece of work involving repeated viewing of the subject(s);
- Is it likely to involve identifying and recording information about third parties such as friends and family members of the subject of interest, or information posted by third parties such as friends or family members, which may include private information and therefore constitute collateral intrusion.

Further guidance; Part 3, paragraphs 3.5 and 3.11-3-16 of the Covert Surveillance and Property Interference Code of Practice 2017
https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice/pages/3/

13 SECURITY AND RETENTION OF DOCUMENTS

13.1 Documents created under this procedure are highly confidential and must be treated as such. Services shall make proper arrangements for their retention, security and destruction, in accordance with the requirements of the Data Protection Act 2018, the General Data Protection Regulation and the Codes of Practice. It should be noted that refusals as well as approved applications must

be retained. The Code of Practice recommends retention of RIPSA records for a period of 3 years.

13.2 Documents will be inspected periodically by the Investigatory Powers Commissioner's Office (IPCO) which has statutory powers of inspection. No records should be destroyed until after they have been inspected by IPCO.

13.3 The original of every authorisation, renewal, refusal and cancellation (including the records relating to oral authorisations) must be passed to the Chief Officer - Legal & Procurement immediately after such authorisation, renewal, refusal or cancellation has been authorised. The Chief Officer - Legal & Procurement shall maintain a central register of all such forms submitted by officers for consideration under RIPSA. In addition, each authorising officer shall maintain a register of current and past authorisations, renewals, refusals and cancellations which shall contain copies of all such completed forms.

13.4 Authorising officers shall ensure that sufficient information is provided to the Chief Officer - Legal & Procurement in order that the Central Register is kept up to date.

14 MONITORING

14.1 Directors shall carry out regular monitoring of directed surveillance and the use of covert human intelligence sources within their Department and review the investigation practices in operation. The Chief Officer - Legal & Procurement shall monitor all submitted authorisations at the time of their submission to him in order to ensure compliance with the provisions of the Regulation of Investigatory Powers (Scotland) Act 2000.

15 ADVICE

15.1 If officers are in any doubt as to whether or not an authorisation is required in respect of a proposed course of action, they should seek advice from a solicitor within Legal Services before engaging in that course of action.

CCTV

If an operator of any Council CCTV system is approached by any other employee or other agency requesting that the operator undertake Directed Surveillance using CCTV, the operator is required to obtain a written copy of a RIPSA authorisation prior to such use. This authorisation must detail the use of a specific camera system for the purpose of directed surveillance. The authorisation must be signed by either one of the Council's Authorising Officers or in the case of the Police, an officer of at least the rank of Superintendent. In urgent cases an authorisation approved by a Police officer of at least the rank of

Inspector can be accepted. A copy should be kept and the original forwarded to the Chief Officer – Legal and Procurement for noting in the central register.

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

DOCUMENTS

This procedure uses the following **forms**, copies of which are available from Legal Services and on the intranet for use by all departments.

1. Application for Authority to Carry Out Directed Surveillance

   This should be completed by the applicant in all cases. The authorisation is effective for three months from the time that approval is given.

2. Review of a Directed Surveillance Authorisation

   The authorising officer should complete this on the date indicated in the original authorisation, the last review, or the renewal.

3. Application for Renewal of Directed Surveillance Authorisation

   The applicant in all cases should complete this where surveillance is required beyond the previously authorised period (including previous renewals).

4. Cancellation of a Directed Surveillance

   The authorising officer should complete this immediately the authorisation ceases to be either necessary or appropriate

5. Oral Record of Authorisation of Directed Surveillance

   This is a record of an oral authorisation, which should be completed by the applicant. It should be used only in cases where the urgency of the situation makes the submission of a written application impractical. The original authorising officer should countersign it as soon as is practicable. This should be annexed to the formal application for authorisation.

6. Application for Authority to Use a Covert Human Intelligence Source

   This should be completed when seeking to use a covert human intelligence source. The authorisation is effective for 12 months from the time approval is given.

7. Review of an Authorisation for us of a Covert Human Intelligence Source

   The authorising officer should complete this on the date indicated in the original authorisation, the last review, or the renewal.

8. Application for Renewal of Authorisation for Use of a Covert Human Intelligence Source

The applicant in all cases should complete this where the use of a covert human intelligence source is necessary beyond the previously authorised period.

9. Cancellation of Use of Covert Human Intelligence Source

The authorising officer should complete this when the authorisation ceases to be either necessary or appropriate.

10. Oral Record of Authorisation of Directed Surveillance

11. Oral Authorisation of Use of a Covert Human Intelligence Source

This is a record of an oral authorisation, which should be completed by the applicant. It should be used only in cases where the urgency of the situation makes the submission of a written application impractical. The original authorising officer should countersign it as soon as is practicable.