DATA LABEL: PUBLIC

West Lothian Council

COUNCIL EXECUTIVE

REGULATION OF INVESTIGATORY POWERS – POLICY REVIEW

REPORT BY DEPUTE CHIEF EXECUTIVE

A. PURPOSE OF REPORT

To consider draft revised Policy, Procedure and Guidance in relation to the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA)

B. RECOMMENDATIONS

1. To approve the revised Policy in relation to the Regulation of Investigatory Powers (Scotland) Act 2000, contained in the appendix
2. To note the terms of the draft revised Procedure and Guidance, also in the appendix, which will support compliance with legislation and with the revised policy

C. SUMMARY OF IMPLICATIONS

I	**Council Values**	Being honest, open and accountable
II	**Policy and Legal (including Strategic Environmental Assessment, Equality Issues, Health or Risk Assessment)**	Regulation of Investigatory Powers (Scotland) Act 2000, statutory Codes of Practice and Guidance; RIPSA Policy and Procedure (2020)
III	**Implications for Scheme of Delegations to Officers**	None
IV	**Impact on performance and performance Indicators**	None
V	**Relevance to Single Outcome Agreement**	N/A
VI	**Resources - (Financial, Staffing and Property)**	None
VII	**Consideration at PDSP**	Public & Community Safety PDSP, 27 April 2023, where no comments were noted
VIII	**Other consultations**	Governance Manager; Chief Solicitor; Environmental Health/Trading Standards; Housing

Customer & Building Services; Operational Services; Audit, Risk & Counter Fraud Team

D. TERMS OF REPORT

1 Background

1.1 The council has duties and responsibilities when undertaking certain types of surveillance in relation to the detection of crime, public safety and the protection of public health. These are found principally in the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA). The legislation provides that in certain circumstances a formal authorisation is needed from an appropriate senior council officer before some forms of information-gathering activity can be carried out. The council's current Policy was approved at Council Executive on 6 October 2020. It is supported by internal procedures, guidance and suite of forms to help council officers who may require authorisation as well as those who determine if authorisation should be granted. All are due for review in 2023/24.

1.2 The Policy lists the roles and responsibilities of all officers engaged in RIPSA activity. Those were approved alongside the current Policy. They are reflected in the Scheme of Delegations to Officers. The Senior Responsible Officer (SRO) is the Depute Chief Executive (Corporate, Housing & Operational Services). The Authorising Officers (AO) are the Governance Manager and the Chief Solicitor. Advice is provided when required by Legal Services. No changes are proposed to that allocation of responsibilities.

1.3 The RIPSA regime is about controlling the way public bodies use their existing statutory powers. It is there to balance the public interest in enforcement against private interests and privacy rights. A RIPSA authorisation does not confer additional or wider powers on the council that it does not otherwise possess. It regulates and controls the way in which existing powers are used. It provides protection for members of the public and not a threat.

2 Policy, Procedure & Guidance

2.1 As required by law, guidance and best practice, the council must have a RIPSA policy together with supporting procedures and guidance. The council's approach requires a full review every three years, timed to coincide with the pattern of statutory inspections by the Investigatory Powers Commissioner's Office (IPCO). The latest inspection took place in November 2022. The inspection report and resulting action plan were reported to Public & Community Safety PDSP on 23 February. Progress on the actions was reported there on 27 April 2023 along with the draft revised Policy, Procedure and Guidance for consideration.

2.2 The draft revised Policy, Procedure and Guidance are in the appendix. The Policy requires approval by elected members. The Procedure and Guidance, as operational matters, are reported to members for information and are kept up to date by officers. The Procedure and Guidance are in turn supported by a suite of forms to be used for applications and authorisations. Those have been updated but have not been produced with this report

2.3 The changes proposed are not extensive or material. The IPCO Inspector found the current documents to be comprehensive and fit for purpose, subject to some minor updates and amendment. The changes implement the relevant post-inspection actions. The most significant changes to note (highlighted in yellow in the appendix) are as follows:-

- Addition of a decision-making chart, as part of the Checklist, to help officers decide if an authorisation may be required (Procedure and Guidance, Part D)

- Addition of an express duty on Heads of Service to ensure there are safeguards in their service area against the risk of "status drift" in relation to Convert Human Intelligence Sources (CHIS). Status drift may occur when a series of interactions with the same individual result in a move from the provision of information on a voluntary and undirected basis to a planned and directed course of actions whereby the individual is subject to council control and direction. Consideration was given to designing and imposing some form of uniform corporate procedure. That was felt to be disproportionate, given the low level of use of covert surveillance methods and the divergence in working arrangements and case management across services (Procedure and Guidance, A3.4). The risk can be adequately addressed through training, the correct use of the Procedure and Guidance, and appropriate advice to Heads of Service

- Addition of an express duty on Heads of Service to ensure there are safeguards in their area to ensure that online research is carried out in a way that does not engage RIPSA. Even online sources open to the public may contain private information. The same rules about covert surveillance apply there as apply to physical surveillance. Initial and limited use is acceptable, but planned, directed and repeated monitoring may require an authorisation. Again, consideration was given to designing and imposing a uniform corporate procedure. That was felt to be disproportionate for the same reasons given in relation to status drift, above (Procedure and Guidance, A4.9). As with status drift, the risk can be adequately addressed through training, the correct use of the Procedure and Guidance, and appropriate advice to Heads of Service

- A restructuring of the definition of "surveillance" and related terms in the Terminology section, to address some scope for confusion identified by the IPCO Inspector (Procedure and Guidance, E16)

E. CONCLUSION

Approval of the draft revised Policy and consideration of the revised Procedure and Guidance will contribute to the council's compliance and monitoring arrangements, to the control of the risk in the corporate risk register, and to the transparency expected in relation to such a significant regulatory regime.

F. BACKGROUND REFERENCES

Public & Community Safety PDSP, 23 February 2022 and 27 April 2023

Appendices/Attachments: 1. Draft revised Policy, Procedure and Guidance

Contact Person: James Millar, Governance Manager/Monitoring Officer, 01506 281613, james.millar@westlothian.gov.uk

Graeme Struthers, Depute Chief Executive (Corporate, Housing and Operational Services)

Date of meeting: 23 May 2023

REGULATION OF INVESTIGATORY POWERS

POLICY, PROCEDURE AND GUIDANCE

(2023)

The policy was approved at Council Executive on 19 September 2017. It is to be formally reviewed every three years. Changes require committee approval other than minor administrative changes or updates. An annual report is to be made to members in relation to RIPSA activity. The Procedure does not require committee approval. It represents management guidelines and so can be amended and updated without reference to members.		
19 September 2017	Policy approved	Immediate effect
21 September 2017	Procedure and guidance finalised and notified to relevant services	Immediate effect
5 October 2018	Annual report to PDSP. Procedures reviewed by officers. Minor changes to terminology, committee approval not required	Immediate effect
23 August 2019	Annual report to PDSP. Procedures reviewed by officers. Adjustment to reporting requirements. Insertion of guidance on internet and social media use. Committee approval not required	Immediate effect
6 October 2020	Council Executive - amendments to Section 5 of the Policy and Section 3 of the Procedure (CHIS); amendments to Section 4.5 of the Procedure (online activity); Policy and Procedure to be subject to triennial review	Immediate effect
23 May 2023	Updates and amendments in relation to post-inspection Action Plan and triennial review, per Public & Community Safety PDSP, 23 February 2023 and 27 April 2023	

CONTENTS

Page

POLICY

1	Aims and objectives	2
2	Roles and responsibilities	2
3	Scope	3
4	Procedures and guidance	4
5	Covert human intelligence sources (CHIS)	5
6	Complaints	5
7	Review and reporting	5

PROCEDURE AND GUIDANCE

A	INTRODUCTION	7
1	Background	7
2	Non-RIPSA activity	7
3	RIPSA activity not covered by this Procedure	7
4	Internet and social media	8
5	Using the procedure and guidance	10
B	PROCESS	10
1	Introduction	10
2	Before starting	10
3	The application	11
4	Emergency applications	12
5	Decision-making	12
6	Authorisation	12
7	Making changes	13
8	Review and renewal	13
9	Cancellation	13
C	GUIDANCE	14
1	Can an authorisation be given at all?	14
2	Is an authorisation actually required?	14
3	Is there a lawful purpose (core function)?	15
4	Is the surveillance necessary?	15
5	Is the proposed surveillance proportionate?	15
6	Will the planned surveillance be effective?	16
7	What information is going to be acquired?	16
8	What do you want to do?	16
9	Things the surveillance should be planned to avoid	17
D	CHECKLIST AND RIPSA DECISION CHART	17
E	TERMINOLOGY	18
F	CONTACTS	20

POLICY

1 Aims and objectives

1.1 In carrying out regulatory or enforcement functions the council may have to gather information through observation without the knowledge of the person involved. Activities like that may involve encroaching on human rights to respect for private life, home and possessions. Doing so can be justified in human rights terms. It must be accordance with law, it must be necessary in the pursuit of a legitimate public aim, and it must be proportionate. To ensure that is the case the council has to follow UK and Scottish legislation (RIPA and RIPSA), Codes of Practice and statutory guidance.

1.2 To meet those requirements the council must have a policy, procedure and guidance; a clear allocation of responsibilities for compliance and internal monitoring; and public reporting arrangements.

1.3 This policy is designed to provide the framework of principles and guidance which the council and its officers must apply when gathering information in certain circumstances using their statutory powers. It provides the basis for procedural rules and guidelines to be followed in the performance of those functions.

1.4 Council officers may be able and permitted to carry out this type of activity. Before doing so they must be authorised properly. As well as complying with legal rules, they must abide by this policy and use correct procedures. That will ensure respect for human rights, public accountability and that information gathered can be used lawfully.

1.5 The policy aims are:-

- to ensure the council acts lawfully in gathering information to the protect the public, safeguard public health or detecting crime
- to protect the legitimate interests of anyone who is being investigated
- to provide a balance between using investigatory powers to serve the community of West Lothian and safeguarding the public against unjustified and unlawful intrusion into their affairs
- to provide the framework for procedural rules and controls
- to make adequate internal monitoring and public reporting arrangements

1.6 The terminology used is explained in Section 8.

2 Roles and responsibilities

2.1 The council will designate a member of its Corporate Management Team to be the Senior Responsible Officer (SRO) who is responsible for:-

- ensuring the council complies with the law, Codes of Practice and other statutory guidance
- maintaining and reviewing the policy
- ensuring officers comply with this policy and related procedures and guidelines
- establishing and reviewing internal procedures and guidance
- providing training
- dealing with the Investigatory Powers Commissioner's Office (IPCO)in relation to oversight and inspection and actions arising
- notifying the Monitoring Officer of any unauthorised surveillance activity
- reporting to PDSP and/or committee on activity under the policy

- completing a certificate of compliance as part of the annual report on the Local Code of Corporate Governance if required by the Monitoring Officer
- appointing a depute to act when the SRO is unable to do so

2.2 The council will designate at least one officer to be the Authorising Officer (AO) who is responsible for:-

- giving, reviewing, renewing and cancelling authorisations
- maintaining a register of authorisations
- notifying the SRO and the Monitoring Officer of any unauthorised surveillance activity
- assisting and supporting the SRO
- providing or arranging the provision of training

2.3 The Chief Solicitor, personally or through nominated solicitors, is responsible for:-

- providing legal advice to the SRO, the AO and other council officers
- assisting and supporting the SRO and AO
- acting as AO when the AO is unable to do so
- notifying the SRO, the AO and the Monitoring Officer of any unauthorised surveillance activity

2.4 The delegation of those powers to officers shall be recorded in the Scheme of Delegations to Officers.

2.5 Heads of Service are responsible for:-

- raising awareness of the policy and procedures and ensuring officers undertake adequate training
- designating and authorising officers to apply for authorisations and carry out and supervise the surveillance as authorised
- informing the AO of the officers designated to apply for authorisations and carry out and supervise the surveillance as authorised
- ensuring compliance with the policy and procedures and any authorisations issued
- notifying the SRO and the AO of any unauthorised surveillance
- assisting and supporting the SRO

2.6 All council officers engaged in surveillance or with responsibilities under this procedure are responsible for:-

- being familiar with the policy and procedure
- complying with the policy and procedure and authorisations issued
- undertaking appropriate training

2.7 IPCO oversees all public bodies engaged in covert surveillance. Part of their role is to periodically examine and audit records and procedures. All council officers engaged in the process must be prepared to justify their actions when called upon to do so. During periods of inspection, all officers must make themselves available for interview and otherwise cooperate with the visiting representative of IPCO.

3 Scope

3.1 The policy applies to council officers who are engaged in:-

- covert surveillance which is directed surveillance

- the use of a covert human intelligence source (CHIS)

3.2 In certain circumstances, those functions may include:-

- the use of CCTV (for example, where deliberate use of those cameras is part of a planned surveillance operation)
- the use of the internet and social media for the purpose of gathering information (for example, where monitoring of a website or social media page is undertaken systematically and over a period of time to gather information)
- test purchasing (for example, where young people are engaged to attempt to make what would be illegal purchases of alcohol or tobacco)

3.3 The policy does not apply to:-

- overt surveillance
- *ad hoc* surveillance
- unplanned surveillance
- purely internal observation in the council's role as employer where there is no surveillance in a public place (for example, disciplinary investigations where ICO guidelines will apply)

3.4 The policy does not permit intrusive surveillance. Council officers must not engage in that activity.

4 Procedures and guidance

4.1 The SRO will put in place appropriate procedures and guidance to ensure that officers act lawfully and in accordance with the policy. Those procedures will be reviewed at least once every three years to coincide with the completion of actions required following triennial IPCO inspections.

4.2 The procedure and guidance shall be designed to ensure that officers consider and satisfy the AO that:-

- the authorisation is legally possible (the council cannot authorise intrusive surveillance)
- the authorisation is legally required - not all observation activity will come within the definition of surveillance requiring an authorisation (for example, overt surveillance)
- the type of information to be gathered has been identified (for example, the involvement of private information and/or confidential information)
- there is a lawful purpose ("core function") (that is, preventing or detecting crime or disorder; public safety; or protecting public health)
- the surveillance is necessary (it is a reasonable way to gather the information, with alternatives having been considered)
- the risk of collateral intrusion has been assessed and mitigating measures put in place
- the proposed surveillance will be effective
- the activity has been planned to avoid damage to property and harassment or intimidation of individuals
- the surveillance activities proposed are proportionate to the conduct being investigated
- competent officers are identified and available to carry out and supervise the surveillance and the subsequent retention and destruction of information

4.3 The procedures shall ensure that:-

- applications, authorisations and related documents and records are normally in writing
- the circumstances in which oral applications and authorisations can be used are clearly defined
- the ability to use social media and other online activity for gathering information is clearly explained
- forms are in place to ensure that the legal requirements and all relevant factual information is considered throughout the process
- authorisations are reviewed, renewed or terminated as required by the circumstances of the case
- a register is kept in compliance with legal requirements
- records are retained and destroyed in accordance with the council's Records Management Policy and Retentions Schedules

5 Covert Human Intelligence Source (CHIS)

5.1 The use of a covert human intelligence source will be authorised only in exceptional circumstances. The council will avoid the use of a CHIS expect in such exceptional circumstances.

5.2 Additional safeguards will be required in considering a request for CHIS authorisation. The procedures shall in particular ensure:-

- that any risk of activity falling into that category is identified and avoided
- that authority is only sought with the express approval of the relevant Head of Service
- that authorisation is not given until full discussion has taken place amongst the SRO, the AO, the Head of Service and the officer requesting the authorisation

5.3 The procedures and guidance shall also address the risk of "status drift", whereby a series of actions taken involving the same individual in providing information in an investigation leads to the use of a CHIS without conscious decision or awareness, and so without an application and authorisation so to do.

6 Complaints

6.1 Any person aggrieved by the granting of an authorisation or by surveillance activity may lodge a complaint to the council under its Corporate Complaints Procedure.

6.2 Any person aggrieved by the conduct of any covert surveillance also has a right to complain to the Investigatory Powers Tribunal. This independent tribunal has full powers to investigate and decide cases within the United Kingdom, including complaints about activities carried out under Scottish legislation.

7 Review and reporting

7.1 This policy shall be reviewed at least once every three years to coincide with the completion of actions required following triennial IPCO inspections. The outcome of the review shall be reported to PDSP. In the event that any changes are required, those changes shall be reported to Council Executive for approval.

7.2 Minor changes required for administrative reasons may be made to the policy by the SRO (for example, to reflect changes in the council's management structure and responsibilities, or changes in terminology).

7.3 The procedures and guidance shall be reviewed every three years by the SRO to coincide with the completion of actions required following triennial IPCO inspections.

7.4 Annual reports will be made by the SRO to PDSP on all activity under the policy and in relation to inspection reports. Should RIPSA activity increase significantly then more frequent reports will be made. Breaches of the law or procedure or complaints or litigation may require *ad hoc* reports.

7.5 If requested, the SRO shall provide a compliance statement to the Monitoring Officer as part of the annual report on the Local Code of Corporate Governance, detailing the extent of surveillance activity during the year and identifying any areas of weakness or concern and non-compliance.

PROCEDURE AND GUIDANCE

A INTRODUCTION

1 Background

1.1 The council has approved a Policy on using the regulation of investigatory powers legislation (RIPSA). The Policy is the council's framework of RIPSA principles and guidance and sits above this Procedure. The Procedure must be followed in all RIPSA cases. It is intended as a practical guide to making a RIPSA application in the case of directed surveillance. It does not apply to CHIS or to intrusive surveillance. Additional safeguards are required for a CHIS authorisation and the council policy is to avoid its use and only to authorise it in exceptional circumstances.

1.2 Directed surveillance can only take place under a RIPSA authorisation. That can only be given by a designated Authorising Officer (AO). The AO is your first point of contact in relation to any proposed application. They will provide advice and guidance in relation to the proposed surveillance and consider your draft application prior to determining whether surveillance should be authorised. The AO contact details are at the end of the Procedure.

1.3 Surveillance is an extremely powerful tool. It must be treated and used with respect, only in accordance with the legislation, and in circumstances which merit such significant measures.

1.4 Granting or refusing an application for authorisation is at the sole discretion of the AO. An application will only be granted where it meets the necessary statutory criteria. Surveillance should always be the last resort and will only be permitted where there are no other means by which to secure evidence, or where all other means by which to obtain evidence have been exhausted without success or else considered but discounted for good reason.

1.5 Part D has a checklist and decision-making chart to help officers determine if RIPSA is engaged and whether an application and authorisation will be required.

2 Non-RIPSA activity

2.1 The AO may take the view that the planned action is not for one of the three lawful purposes (core functions), and that may result in them refusing the application. The AO may also take the view that what is being planned is not directed surveillance, or is not covert surveillance, and so might refuse the application. However, activity that is not covered by the RIPSA legislation may still be lawfully carried out and the planned activity may in some cases still take place. An example is test-purchasing in relation to under-age sale of tobacco or alcohol, which, depending on the means employed and adherence to relevant professional guidelines, may not require an authorisation.

3 RIPSA activity not covered by this Procedure

3.1 The council is not authorised to use intrusive surveillance under any circumstances.

3.2 It would be exceptional for the Council to use Covert Human Intelligence Sources (CHIS). CHIS is the subject of particular provisions within the legislation. If you are considering the need for CHIS then you should consult an AO who will be able to discuss matters with you in detail. The use of covert human intelligence sources will only be authorised in exceptional circumstances and with additional safeguards in place. Authorisation for CHIS may only be requested with the express approval of your Head of Service. CHIS authorisation will not be given until full discussion has taken place amongst the SRO, the AO, the Head of Service and the officer seeking authorisation.

3.3 In relation to a CHIS, "status drift" may occur when a series of interactions with the same individual result in a move from the simple acquisition and provision of information on a voluntary and undirected basis to a planned and directed course of actions whereby the individual is subject to council control and direction. You should be alert to that danger when engaging more than once or twice with the same individual about the same subject as part of the same investigation. If a pattern of recurring and repeated interaction emerges then take advice from the AO.

3.4 Heads of Service are responsible for ensuring that consideration is given by officers to the risk of status drift. The RIPSA decision-making chart in Part D should be consulted. Factors to consider include frequency and regularity of contact, the way in which information may be gathered, the extent of direction or guidance form officers in determining the information to be acquired and the means of doing so. An appropriate record of that consideration and its conclusion must be kept. The risk should be reviewed periodically throughout the investigation.

4 Internet and social media

4.1 Intelligence and information is readily available on the internet and social media. It may include information of significant value in pursuing statutory powers. Recording and using personal data from those sites may engage the Data Protection Act 2018. Viewing websites and social media sites is likely to interfere with individuals' rights to the enjoyment of their private life and expectations of privacy. In the same way, an individual may have a reduced expectation of privacy when in a public place but still covert surveillance may result in the acquisition of private information relating to the individual concerned or collateral intrusion.

4.2 Despite the sites being publicly available and freely accessible, and regardless of security/access settings applied to the site, visiting those sites may also require a RIPSA authorisation depending on the activity undertaken. Such sites, even when they are on the face of it designed for commercial purposes, may contain private information relating to the owner or operator of the site and their family or associates.

4.3 Use of the internet for information gathering prior to an investigation should not engage privacy considerations or require an authorisation. That is not necessarily restricted to just one instance of information gathering, or two, or any set number. The test is whether it falls within the definition of covert directed surveillance for one of the three statutory purposes for RIPSA ("the core functions").

4.4 The use of some sites by individuals may carry a greater or lesser expectation of privacy, depending on the information available and the generally understood purpose of the site and its use. Care is required where even an apparent commercial site might nevertheless carry or enable access to personal or private information unrelated to the commercial purposes.

4.5 Accessing sites overtly will not require a RIPSA authorisation. Use which clearly discloses the access is by the council or on the council's behalf, or where notice is given that monitoring will take place, is not covert activity, regardless of whether it amounts to surveillance. Use of an anonymised or fake or false identities or profiles will mean an authorisation is required if the definition of directed surveillance for core functions is met.

4.6 Use of the internet for non-core functions does not require an authorisation but the council's Information Governance Policy and its related Procedures will govern that use.

4.7 The Scottish Government Code of Practice (2017)[1] describes circumstances in which online activity may lead to the requirement for an authorisation. Those include;-

- Your intention to engage with others online without disclosing your identity
- The likelihood of the subject of the surveillance being aware of it taking place
- Accessing social media sites used for either or both of personal or business reasons as opposed to accessing publicly available online databases
- The systematic collection and storing of information about an individual or group as opposed to an initial information-gathering reconnaissance

4.8 The Code also lists factors to consider in determining if online activity requires an authorisation, including:-

- The likelihood of obtaining private information about a person or group of people
- Visiting internet sites to build up an intelligence picture or profile
- Recording and storing the information obtained
- The likelihood of providing an observer with a pattern of lifestyle
- Combining the information acquired with other sources of information or intelligence, which amounts to information relating to a person's private life
- The activity is part of an ongoing piece of work involving repeated viewing of the subject(s)
- The involvement of identifying and recording information about third parties, or information posted by third parties, which may include private information and therefore constitute collateral intrusion

[1] https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice/

4.9 Heads of Service are responsible for ensuring that consideration is given by officers when starting work on a new investigation to the risk of undertaking online research in a manner and to an extent which engages RIPSA and requires an application and authorisation. The RIPSA decision-making chart in Part D should be consulted. Factors to consider include any ongoing work in relation to the same matter or the same individuals; the rationale and justification for using online tools; the intended frequency of monitoring the same sources or applications; the way in which information acquired will be recorded and used. An appropriate record of that consideration and its conclusion must be kept.

4.10 The Information Governance Policy governs the setting up or registering of websites or social media accounts or profiles. Establishing and using fake, false or anonymised accounts may only be done with the agreement of the SAO. That will be given subject to conditions on the officers who may use them, how they may be used and the records to be kept of their use.

5 Using the procedure and guidance

5.1 The Procedure is in six parts:-

A. Introduction - this section setting the RIPSA scene

B. Process - the mechanics of making the application and what happens afterwards

C. Guidance - help in addressing all the relevant information required by the application form

D. Checklist - an *aide memoire* and decision-making chart to help last-minute checks, revisions and amendments to the application and review forms

E. Terminology - definitions and explanations of words and phrases used in RIPSA cases

F. Contacts - information about the Senior Responsible Officer and the Authorising Officers

B PROCESS

1 Introduction

1.1 The Policy sets out the roles and responsibilities held by everyone involved in using RIPSA. You have responsibilities too. Make sure you understand what they are before taking or planning any action or application.

1.2 Everything done by anyone in relation to RIPSA must be done in accordance with legislation, Codes of Practice, the council's Policy and this Procedure, and having regard to Codes of Practice.

1.3 Consult the checklist and decision-making chart in Part D.

2 Before starting

2.1 You must be familiar with and understand the Policy and the Procedure.

2.2 You must have undertaken appropriate training.

2.3 You must have a general authorisation from your Head of Service to take on responsibilities under the Policy and Procedure.

2.4 You must have agreement from your Head of Service to proceed with the application.

2.5 You must let the AO know that an application is being prepared and when the surveillance is intended to start. The AO will need time to make a decision and will have other work to take into account.

2.6 You should discuss the case informally with the AO to make sure the application is covered by the legislation and is one that can be granted

3 The application

3.1 In almost all cases, an application can be prepared and submitted well in advance of the surveillance starting. In exceptional cases there may not be time to complete and submit an application before the surveillance has to begin. These situations are extremely rare. The procedure for those is explained below.

3.2 For normal, non-urgent cases, ask the AO for a Unique Reference Number (URN). The URN will be used in all correspondence and in the Register kept by the AO.

3.3 Familiarise yourself with the application form and what is required.

3.4 Use the Guidance later in this Procedure to help you fill out the form.

3.5 Draft the application carefully and revise it before submitting it. You may attach other documents where appropriate, for example, a map or plan showing proposed surveillance points. Mark them with the URN and the date.

3.6 The form is detailed and appears repetitive. However, each section has a specific function. It is necessary to provide detailed information appropriate to that section, regardless of whether it also appears elsewhere in the form.

3.7 If you have time, ask a colleague or your line manager to review the application.

3.8 Consult the checklist in the Guidance to make sure you have included everything that you should have.

3.9 Follow any instructions given by your line manager - for example, having it signed off by someone else before it goes. The AO will assume that those internal processes have been followed properly.

3.10 Make sure to submit the application in enough time for a decision to be made before the expected start of the surveillance.

3.11 The content of the application is your responsibility. Whilst assistance may be provided, you hold all of the information regarding the circumstances which will support your request for authorisation. Your application will contain all information supporting your request for authorisation. You must provide enough information to satisfy the AO that all the relevant factors have been thought through and are explained. The AO will not make assumptions about what you may have meant to say in your application. You should be prepared to discuss the proposed surveillance in detail with the AO.

3.12 Sign the application, date it, scan it and send it to the AO by email.

4 Emergency applications

4.1 In exceptional cases there may not be time to complete and submit an application before the surveillance has to begin. These situations are extremely rare.

4.2 In an urgent case, a verbal application may be made to the AO and may be granted for up to 72 hours. The urgency should relate to the subject of surveillance and not, for example, to delays in making the application.

4.3 If you consider that you require an emergency authorisation you should immediately contact the AO. The AO will assign a URN and enter the application in the Register. You should keep a note of what surveillance activity is being authorised.

4.4 You must follow up the verbal authorisation with a written application following the procedure set out above.

4.5 If you do not submit a written application on time the verbal authorisation will run out and be cancelled. The AO will confirm the position.

4.6 You will be instructed to immediately cease surveillance activity and remove any surveillance equipment.

5 Decision-making

5.1 The AO may seek more information from you before making a decision. That will usually mean amending the application to ensure that all the necessary information is included.

5.2 The AO may refuse the application. The reasons for refusing it will be explained.

5.3 The AO may grant the authorisation. They will sign it and date it, retain it and send you a copy.

5.4 You cannot begin your surveillance operation until you have confirmation that your application has been granted. You do not need to have the signed authorisation in your hand to begin the surveillance. However, you must have been told that it has been granted.

5.5 The AO will mark the Register to show the decision made and the date.

6 Authorisation

6.1 You must retain a copy of the authorisation provided to you by the AO.

6.2 The authorisation is valid for 3 months but it will be subject to a review before that and may also be cancelled before the end of that period.

6.3 The date for review will depend on the circumstances. The review date may have been discussed and agreed with the AO as part of the application process. If not, the AO will determine an appropriate review date.

6.4 You must comply with the authorisation and do all that you can to ensure that others do so as well. That includes keeping written records of surveillance activity carried out (when, where, by who) and information gathered.

6.5 You must follow any internal arrangements put in place by your line manager or Head of Service, such as providing periodic progress reports.

6.6 You cannot begin your surveillance operation until you have confirmation that your application has been granted. You do not need to have the signed authorisation in your hand to begin the surveillance. However, you must have been told by the AO that it has been granted. In most cases you will receive confirmation by phone and/or email. This will be followed by a copy of the authorised application.

7 Making changes

7.1 After starting the surveillance it may be that something has to be changed. For example, it may be that a different officer will have to carry out the surveillance activity; the location from which the surveillance is being carried out might have to be changed; it might be necessary to use some equipment that was not covered by the authorisation. You must contact the AO to explain the necessary change and to justify it.

7.2 If the AO decides that the change is significant then the authorisation will be cancelled and a fresh application submitted and authorised.

7.3 If the AO decides that the change is not significant then a change may be made to the existing authorisation and recorded by you and the AO as an addition to that authorisation.

7.4 Approval by the AO is needed before you proceed under any new arrangements.

8 Review and renewal

8.1 The review process is to reconsider the authorisation, whether it is still appropriate for it to be in place and for surveillance to continue. A renewal can only be given before the authorisation ends.

8.2 Before the review date you must consider and assess any evidence gathered as a result of the surveillance.

8.3 At least four days before the review date you must submit a review form to the AO. It must explain the evidence gathered, state whether the surveillance requires to continue and why. It is your responsibility to do so.

8.4 If you fail to submit the review form your authorisation will be cancelled. You will be instructed to immediately cease surveillance activity and remove any surveillance equipment.

8.5 Reviews will not be back dated or considered retrospectively.

8.6 The AO may seek more information from you before making a decision. That will usually mean amending the review form to ensure that all the necessary information is included.

8.7 If the AO decides the surveillance is to continue, you will be given a further review date and the process will be repeated.

8.8 If the AO decides that the surveillance is no longer necessary or justified your authorisation will be cancelled.

9 Cancellation

9.1 An authorisation will be cancelled where a written application does not follow a verbal authorisation on time; where a review form is not submitted on time; where you

decide that the surveillance should end; or where the AO decides that the surveillance should end.

9.2 If you decide that the surveillance should be terminated than you must submit a cancellation form. You must do so as soon as it is apparent that surveillance is no longer needed.

9.3 The surveillance operation may be terminated at any time. It is not dependent upon reaching a review date or the expiry of the 3 month period for which the authorisation was granted.

9.4 You must always submit a cancellation form to the AO at the conclusion of the surveillance operation. It forms an essential part of the record keeping requirements. There are NO circumstances in which it would be unnecessary.

C GUIDANCE

1 Can an authorisation be given at all?

1.1 If the proposed surveillance is "intrusive surveillance" then no activity can be authorised. Council officers must not engage in intrusive surveillance.

1.2 Intrusive surveillance is covert surveillance that:-

- is carried out in relation to anything taking place on any residential premises or in any 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

2 Is an authorisation actually required?

2.1 Use the checklist and decision-making chart in Part D.

2.2 No authorisation is needed for:-

- Overt surveillance – gathering information in an open, transparent and unhidden way (for example, observations from a clearly marked vehicle in a public place)
- *Ad hoc* surveillance – a one-off instance of information-gathering through undirected means with no systematic observation planned or carried out (for example, an initial check on a website or social media page)
- Unplanned surveillance – the observation of events as an immediate response to events without planning or forward thinking (for example, coming across information by chance in a public place)
- Surveillance purely internal to the council in its role as employer rather than as a public body (for example, most disciplinary investigations, where information is gathered on council premises or property, although carrying out surveillance of an employee in a public place may mean that authorisation is needed)

2.3 However, authorisation may be need for some activity which does not at first seem to be covert surveillance.

2.4 Authorisation may be required for web-based activities, such as internet searching or accessing social media. This applies even though the subject of the surveillance chooses to make information available in those ways. Generally, a first check and a second follow-up check may be permitted without authorisation. That is more likely to be so if no data is recorded or retained. More frequent or sustained or regular checks or the systematic recording of information will usually mean an authorisation is needed.

2.5 Heads of Service are responsible for putting appropriate procedures in place to ensure that use of the internet and social media which requires an authorisation does not take place without one. Those will be steps in internal service procedures, usually embedded in case management systems or other software. Appropriate records must be kept.

2.6 CCTV footage gathered through general and publicly signposted use will not require an authorisation. However, if it is planned to gather and use it as part of a programme of directed surveillance then it should be covered by an authorisation

3 Is there a lawful purpose (core function)?

3.1 The surveillance must be carried out for a defined lawful purpose or core function, and there are only three:-

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

3.2 Ministers have the power to add to this list. They have not done so.

3.3 You must identify and explain at least one of these three purposes. It must be related to something the council can do lawfully under the legislation applying to the service.

4 Is the surveillance necessary?

4.1 Directed surveillance should be the last resort for gathering information. You must deal with these three issues in the application to show that there are no viable and realistic options available:-

- Is there a reasonable and effective alternative way of achieving the desired objectives in the specific circumstances of the particular case?
- If other methods are available by which the same evidence may be recovered then those alternatives should be applied and exhausted before seeking authorisation.
- If other methods are available by which alternative evidence of similar value may be recovered then those alternatives should be applied and exhausted before seeking authorisation.

5 Is the proposed surveillance proportionate?

5.1 Directed surveillance is a potential infringement of human rights. Part of the legal justification for that is that the infringement is proportionate to the conduct being investigated and the potential harm being prevented.

5.2 These are the points to over in the application form to meet the “proportionality” arguments:-

- Provide relevant and sufficient reasons in support of the application to show later that a fair decision making process was followed and safeguards against abuse were made clear
- Explain the harm being addressed and why the surveillance planned is proportionate in relation to it
- Show that the degree of intrusion upon the target is not excessive
- Satisfy the AO either that collateral intrusion is avoided, or if it cannot be avoided that it has been identified and addressed. That is done through mitigating, minimising, and safeguarding and controlling access to collateral information gathered. There should be controls to identify, separate and securely destroy data gathered in relation to people other than the subject of the surveillance
- Demonstrate that all other reasonable options for gathering the evidence have been considered and rejected for good reason

6 Will the planned surveillance be effective?

6.1 This is a more practical point. Part of justifying the surveillance is showing that it is likely to be effective in gathering evidence that will help the council deal with the misconduct or harm being investigated.

6.2 You should cover these points:-

- What are the prospects of successful recovery of information required in the pursuit of the investigation?
- Are there trained and experienced officers available to carry out the surveillance and supervise it adequately?
- Are the resources available that are required to properly carry out the surveillance and ensure compliance with the authorisation to be given?

7 What information is going to be acquired?

7.1 Consideration must be given to the type of information which may be gathered, in particular if it will be private information or confidential information. Surveillance should be planned in such a way as to avoid such material being obtained.

7.2 If it is possible that such information will be gathered then the application should explain how it will be identified, how access to it will be controlled and how it will be destroyed once it is no longer necessary.

8 What do you want to do?

8.1 You must explain what surveillance actions you wish to undertake.

8.2 If technical equipment is to be used then you must say what it is, how it works, and how it will be used to acquire and record information.

8.3 You must identify where the surveillance will be carried out and describe the location to help show if there may be collateral intrusion or confidential information gathered. Using maps, plans and photographs may be sensible.

8.4 You must say who will be carrying out the surveillance activity and describe their post/position, qualifications, training and experience.

9 Things the surveillance should be planned to avoid

9.1 These are things that should be considered when planning the surveillance. You should show that you have thought about them, and that the planned surveillance either avoids them entirely, or minimises them if they are not avoidable.

9.2 The proposed surveillance activities must be planned to avoid damage to property and harassment or intimidation of individuals

9.3 The risk of collateral intrusion must be considered. This is obtaining information about other persons who are not the subject of the surveillance. Reasonable steps should be taken to avoid or at least minimise that possibility. Where that is likely to happen, steps must be taken to protect that information and ensure it is not retained unless that cannot be avoided.

9.4 A risk assessment should be carried out of the risk of harm to the officers carrying out the surveillance. It should be planned in a way to avoid or at the very least minimise and mitigate those risks.

D CHECKLIST AND DECISION-MAKING CHART

1 Have you identified and explained a lawful purpose (core function) for the activity?

2 Have you fully explained the conduct to be authorised?

3 Are the grounds for necessity correct?

4 Have you detailed why the activity is necessary?

5 Have you detailed why the activity is proportionate?

6 Have you explained what it is desired to achieve from the activity?

7 Have you detailed potential collateral intrusion, and why it is unavoidable?

8 Does the application provide evidence of efforts to reduce collateral intrusion if possible?

9 Is it likely confidential information will be obtained and is it unavoidable?

10 Does the application provide evidence of efforts to deal with confidential information?

11 Have you been able to verify and understand fully the reliability of the information provided to support the application?

12 If technical equipment is being used, do you understand and have you explained its capability enough to estimate what it will capture, and therefore how intrusive it might be?

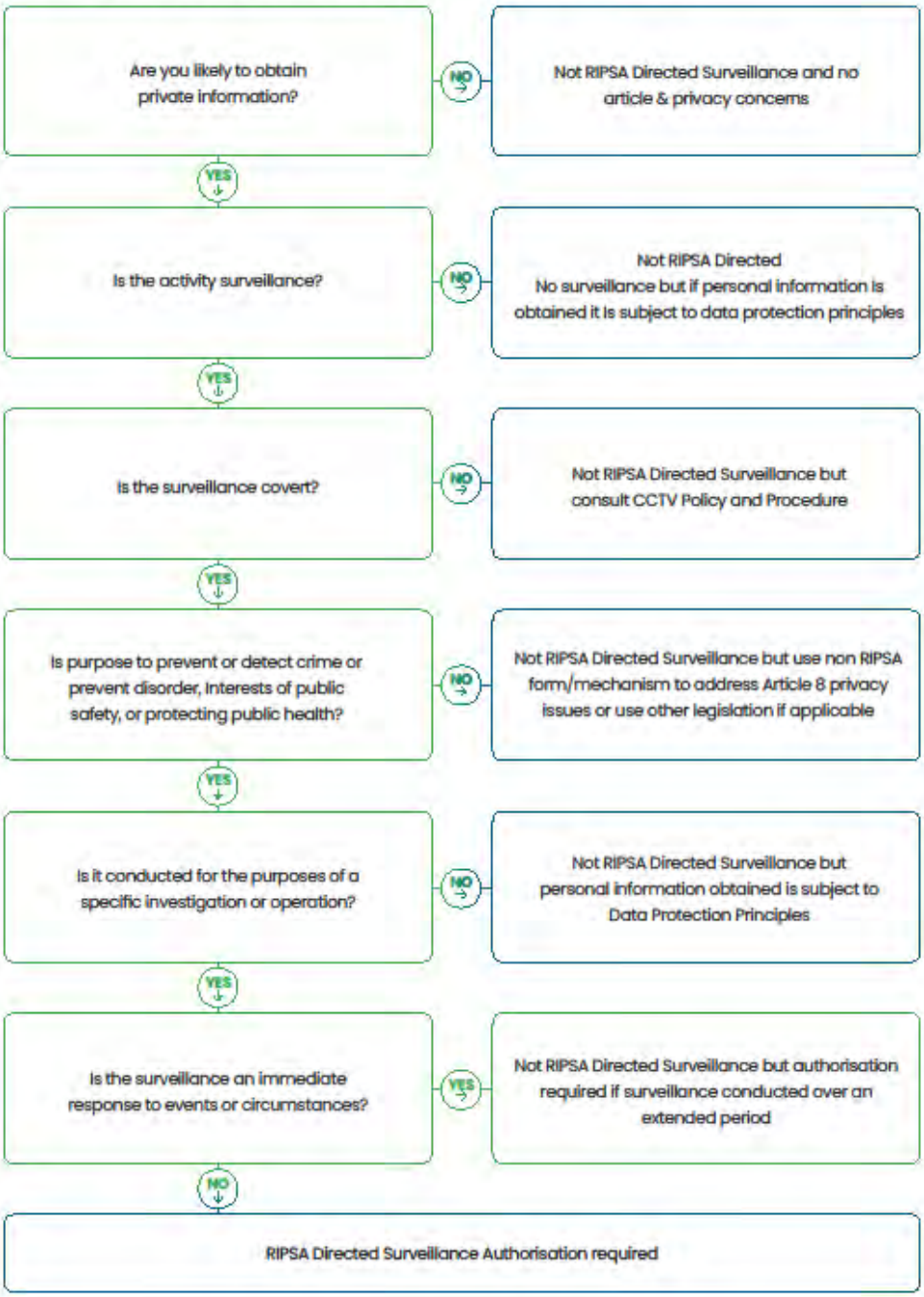
13 Have you checked to ensure the activity will not interfere with other operations being conducted?

14 Have you covered who, what, why, where, when, and how?

15 Advice can be requested from the Authorising Officers. Ask in plenty of time!

Appendix 1

RIPSA Directed Surveillance Decision Chart



E TERMINOLOGY

1	*Ad hoc* surveillance	A one-off instance of information-gathering through undirected means with no systematic observation planned or carried out (for example, an initial check on a website or social media page)
2	Codes of Practice[2]	Statutory Codes of Practice and Guidance issued by the UK Government, the Scottish Government or IPCO
3	Collateral intrusion	Through the authorised surveillance activity, obtaining information about other persons who are not the subject of the surveillance
4	Core functions	The specific grounds set out in statute or Codes of Practice for which an authorisation may be required. "Non-core functions" is construed accordingly
5	Council Executive	The council's main decision-making forum for non-education business established under the council's Standing Orders for the Regulation of Meetings and Scheme of Administration
6	Information Governance Policy	The council's umbrella policy covering the acquisition, use, sharing, disclosure and retention of all information used by the council in pursuit of its public or private powers and duties (Council Executive, 25 June 2019)
7	Investigatory Powers Tribunal	PO Box 33220, London, SW1H 9ZQ Tel: 0207 035 3711 Email: info@ipt-uk.com
8	IPCO	The UK RIPSA and RIPA regulatory body, the Investigatory Powers Commissioner's Office, PO Box 29105, London, SW1V 1ZY
9	Non-core functions	See core functions
10	Officers	Council employees or others authorised by the council to carry out functions or provide services on its behalf and under the direction of the Chief Executive
11	PDSP	The Public & Community Safety Partnership & Resources Policy Development & Scrutiny Panel established under the council's Standing Orders for the Regulation of Meetings and Scheme of Administration
12	Private information[3]	In relation to a person, it includes any information relating to the person's private or family life.
13	RIPA	Regulation of Investigatory Powers Act 2000
14	RIPSA	Regulation of Investigatory Powers (Scotland) Act 2000

[2] RIPSA, sections 24 - 26
[3] RIPSA, section 1(9)

15	Scheme of Delegations	The council's record of the powers and responsibilities delegated to and exercisable by officers
16[4]	Surveillance[5]	Surveillance includes:- (a) monitoring, observing or listening to persons, their movements, their conversations or their other activities or communications; (b) recording anything monitored, observed or listened to in the course of surveillance; and (c) surveillance by or with the assistance of a surveillance device
	Unplanned surveillance	The observation of events as an immediate response to events without planning or forward thinking (for example, coming across information by chance in a public place)
	Directed surveillance[6]	Covert surveillance which is not intrusive and is undertaken:- (a) for the purposes of a specific investigation or a specific operation; (b) in such a manner as is likely to result in the obtaining of private information about a person (whether or not one specifically identified for the purposes of the investigation or operation); and (c) otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under this Act to be sought for the carrying out of the surveillance
	Overt surveillance	Gathering information in an open, transparent and unhidden way (for example, observations from a clearly marked vehicle in a public place)
	Covert surveillance[7]	Surveillance that:- (a) if, and only if, is carried out in manner that is calculated to ensure that persons who are subject to the surveillance are unaware that it is or may be taking place; (b) is for a covert purpose, that is, in relation to the establishment or maintenance of a personal or other relationship, if and only if the relationship is conducted in manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose; and

[4] The tracked changes are not shown here, but the definitions in this section 16 have been re-ordered for clarity as suggested by the IPCO Inspector in November 2022. This footnote will not appear in the amended document when approved

[5] RIPSA, section 31(2) and subject to the exclusions in section 31(3)

[6] RIPSA, section 1(2)

[7] RIPSA, section 1(8)

	(c) if and only if leads to information used or, as the case may be, disclosed in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the use or disclosure in question
Intrusive surveillance[8]	Covert surveillance that:- (a) is carried out in relation to anything taking place on any residential premises or in any private vehicle; and (b) involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device
Covert Human Intelligence Source (CHIS)[9]	A person:- (a) establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating the doing of anything falling within paragraph (b) or (c) below; (b) covertly uses such a relationship to obtain information or to provide access to any information to another person; or (c) covertly discloses information obtained by the use of such a relationship or as a consequence of the existence of such a relationship
Lawful surveillance	Surveillance if:- (a) an authorisation under this Act confers an entitlement to engage in that conduct on the person whose conduct it is; and (b) that person's conduct is in accordance with the authorisation

F CONTACTS

1 The Senior Responsible Officer is Graeme Struthers, Depute Chief Executive, 01506 281776, graeme.struthers@westlothian.gov.uk. He has an oversight role and is not involved in the authorisation procedure.

2 The Authorising Officers are:-

- James Millar, Governance Manager, 01506 281613, 078670466449, james.millar@westlothian.gov.uk
- Carol Johnston, Chief Solicitor, 01506 281605, 07970 478897, carol.johnston@westlothian.gov.uk

[8] RIPSA, section 1(3), and subject to conditions and exclusions in section 1(4) and (5)
[9] RIPSA, section 1(7) and section 31(5)