East Lothian Council

REPORT TO: Cabinet

MEETING DATE: 13 September 2022

BY: Executive Director for Council Resources

SUBJECT: Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA) Policy

---

1 PURPOSE

1.1 Following an overall positive routine inspection and associated recommendations by the Investigatory Powers Commissioner, the Council's corporate Policy regarding compliance with the Regulation of Investigatory Powers (Scotland) Act 2000 ('RIPSA') has been reviewed and updated.

2 RECOMMENDATIONS

2.1 To approve the Council's updated RIPSA Policy.

3 BACKGROUND

3.1 In the course of their duties, it may be necessary on occasion for Council officers to make observations of an individual (or individuals) without that person's knowledge. By their nature, actions of this sort may constitute an interference with that person's right to privacy and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights ('ECHR') and the Human Rights Act 1998 ('HRA'), i.e. 'the right to respect for private and family life'. RIPSA was enacted to provide a clear statutory framework for the operation of covert surveillance investigative techniques, to provide for compliance with the HRA.

3.2 East Lothian Council is committed to respecting and maintaining citizens' privacy and is fully committed to complying with the HRA. The aim of this Policy is to provide the framework for the Council's process for authorising and managing covert surveillance operations under RIPSA, and to set the parameters for expected good practice.

3.3 On 23 February 2022, the Council underwent a desktop inspection by the Investigatory Powers' Commissioner's Office ('IPCO'), the national

regulator for compliance with the RIPSA framework (RIPA in England and Wales). The inspection was in line with the routine 3-yearly inspection schedule for relevant authorities, and consisted of a video conference interview involving the Inspector, the Council's Senior Responsible Officer (Head of Corporate Support), the RIPSA Gatekeeper (Team Manager-Information Governance) and the Service Manager-Governance. The Inspector provided comments on the Council's RIPSA documentation and asked the Council officers a series of questions, noting that the level of compliance shown by the Council removed the need for a physical inspection.

3.4 The Council received the Commissioner's report on 08 March 2022. The report was positive on the whole, noting a number of points of good practice, including the introduction of a quality assurance process for RIPSA applications and the development of a training programme for relevant Council officers. The Commissioner supported the Council's commitment to reviewing its RIPSA Policy and re-establishing a reporting schedule to elected members regarding compliance with the Policy, and he provided recommendations for revisions to be addressed in the new version of the Policy.

3.5 The Council's existing Policy was approved in 2013 and is due for review to reflect current surveillance practices and updated guidance from the Investigatory Powers Commissioner. The Council also has a separate, but linked, Surveillance through Social Media Policy approved around the same time to govern the use of online information and social media to conduct covert surveillance.

3.6 The new Policy combines the existing RIPSA and Surveillance through Social Media Policies into a single document. The main changes include:

- Roles and responsibilities have been expanded;
- Covert Human Intelligence Sources (CHIS) operations have been addressed in greater detail;
- Distinctions have been clarified between RIPSA-related and non-RIPSA-related forms of surveillance;
- Detailed requirements regarding the capture of information have been removed, with pointers to legal provisions, the Codes of Practice and Council templates to sit within the Council's compliance framework.
- Provisions regarding Records Management have been expanded;
- Provisions for online/social media surveillance have been included and updated in line with recent guidance from the IPCO;
- Forms and other appendices have been removed to be managed separately via the compliance framework.

4 POLICY IMPLICATIONS

4.1 This report requests the approval of the updated RIPSA Policy, which is applicable to all Council staff.

5 INTEGRATED IMPACT ASSESSMENT

5.1 The subject of this report does not affect the wellbeing of the community or have a significant impact on equality, the environment or economy.

6 RESOURCE IMPLICATIONS

6.1 Financial – there are no direct financial implications to this report.

6.2 Personnel – there are no new personnel implications to this report.

7 BACKGROUND PAPERS

7.1 None.

Appendix - RIPSA Policy 2022-2025

AUTHOR'S NAME	Zarya Rathé
DESIGNATION	Team Manager - Information Governance
CONTACT INFO	01620 827989; zrathe@eastlothian.gov.uk
DATE	23/08/2022

EAST LOTHIAN COUNCIL

Regulation of Investigatory Powers (Scotland) Policy

East Lothian Council

CONTENTS **PAGE**

Document Control			
Version	**Date**	**Description**	**Reviewed by**
1.0	05/08/2003	CHIS policy ELC Covert Surveillance Policy	
2.0	23/04/2013	Regulation of Investigatory Powers (Scotland) Policy Surveillance through Social Media Policy	Renate Gertz
3.0	13/09/2022	Regulation of Investigatory Powers (Scotland) Policy 2022-2025. Significant updates include: • Expanded roles and responsibilities; • CHIS addressed in greater detail; • Distinctions clarified regarding RIPSA-related and non-RIPSA-related forms of surveillance; • Detailed requirements regarding the capture of information removed, with pointers to legal provisions, the Codes of Practice and Council templates to sit within the Council's compliance framework. • Expanded section on Records Management; • Inclusion of provision for online/social media surveillance in line with recent guidance from the IPCO. This will now supersede the Council's Surveillance through Social Media Policy. • Forms and other appendices removed to be managed separately via the compliance framework.	Zarya Rathé

1. INTRODUCTION

1.1. This document sets out East Lothian Council's Policy regarding its use of powers under the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA).

1.2. In the course of their duties, it may be necessary on occasion for East Lothian Council employees to make observations of a person or persons in a covert manner, i.e. without that person's knowledge. By their nature, actions of this sort may constitute an interference with that person's right to privacy and may give rise to legal challenge as a potential breach of Article 8 of the European Convention on Human Rights[1] and the Human Rights Act 1998 ('the right to respect for private and family life'). RIPSA was enacted to provide a clear statutory framework for the operation of certain intrusive (in the ordinary sense) investigative techniques, to provide for compliance with the Human Rights Act 1998 (HRA).

2. STATEMENT OF INTENT

2.1. The aim of this policy is to provide the framework for the Council's process for authorising and managing covert Directed Surveillance and CHIS operations under RIPSA, and to set the parameters for expected good practice.

2.2. East Lothian Council is committed to respecting and maintaining citizens' privacy and is fully committed to complying with the HRA. Both RIPSA and HRA impact on the way the Council conducts its business. Amongst other things, HRA entitles citizens to expect that their privacy will be respected in relation to their private life, family life, their home and correspondence. It also entitles them to peaceful enjoyment of their possessions. RIPSA recognises that these rights may, nevertheless, be lawfully infringed in some circumstances provided the method used is lawful, has a legitimate aim, is necessary and is proportional to what it would achieve.

3. OBJECTIVE

3.1. The objective of this Policy is to ensure that all covert surveillance by East Lothian Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the relevant legislation, the Scottish Government's

[1] As of 2022 and the time of this Policy review, the United Kingdom remains committed to respecting the framework of the European Convention on Human Rights following the UK's exit from the European Union ('Brexit'). Any changes to this position in future shall be reflected in this Policy as necessary.

Codes of Practice on Covert Surveillance and Covert Human Intelligence Sources ('the Codes of Practice') and any guidance which the Investigatory Powers Commissioner's Office (IPCO) may issue from time to time.

3.2. This Policy is intended to govern a compliance framework consisting of more detailed measures, templates, forms and guidance that support the Council in achieving this objective.

4. STATUTORY FRAMEWORK

4.1. While this Policy directly addresses the Council's activities under RIPSA, it is recognised that such activities may also be subject to other legal and regulatory regimes, for example the Data Protection Act 2018 / UK GDPR and the Public Records (Scotland) Act 2011. In carrying out covert surveillance, Council employees must have due regard for the requirements of all applicable laws, regulations and codes of practice, and must familiarise themselves with all relevant Council policies and procedures, including (but not limited to) the Data Protection Policy, the Information and Records Management Policy and the IT Acceptable Use Policy.

5. DEFINITIONS

5.1. In this Policy:

'CHIS' and 'Source' mean Covert Human Intelligence Source;

'Codes of Practice' means the Scottish Government's Covert Surveillance & Property Interference Code of Practice (2017) and the Covert Human Intelligence Sources Code of Practice (2017) or any relevant successor Codes of Practice issued by the Scottish Government;

'IPC' and 'IPCO' mean the Investigatory Powers Commissioner and the Investigatory Powers Commissioner's Office, respectively;

'RIPSA' means the Regulation of Investigatory Powers (Scotland) Act 2000;

'2010 Order' means the Regulation of Investigatory Powers (Prescription of Offices, etc. and Specification of Public Authorities) (Scotland) Order 2010;

'2014 Order' means The Regulation of Investigatory Powers (Authorisation of Covert Human Intelligence Sources) (Scotland) Order 2014.

6. ROLES AND RESPONSIBILITIES

6.1. All Staff

All Council staff must familiarise themselves with the definitions of covert surveillance, Directed Surveillance, CHIS, and Intrusive Surveillance. They must also ensure that they understand when authorisation under RIPSA is required.

Responsibilities include:

- Completing role-relevant training via e-learning or face-to-face, as guided by their line manager;

- Asking for further guidance from their line manager and/or the RIPSA Gatekeeper / Coordinating Officer regarding how to maintain compliance with RIPSA and the statutory framework.

6.2. Investigating Officers (IO)

Investigating Officers are the Council officers undertaking covert surveillance operations under RIPSA. In addition to the responsibilities held by all staff, IOs are responsible for:

- Completing and submitting applications for RIPSA authorisation to the Authorising Officer in line with the relevant policies and both statutory and internal guidance;

- Completing and submitting Review, Renewal and Cancellation forms to the Authorising Officer for comment and approval as needed;

- Carrying out the relevant operation/investigation;

- Feeding back to the Authorising Officer regarding any significant changes or developments to the operation;

- Consulting with the Coordinating Officer/Gatekeeper as needed and producing documentation for central registration and storage;

- Ensuring that any product (i.e. information gathered as part of an operation) is managed in line with the Authorising Officer's instructions and with reference to the Council's RIPSA and Information/Records Management policies and procedures.

6.3. Authorising Officers (AO)

Authorising Officers hold a prescribed office, and are responsible for authorising and reviewing applications submitted by Investigating Officers. In addition to the responsibilities held by all staff, they oversee and mitigate surveillance actions by:

- Checking the standard of information provided;
- Stating explicitly what is being authorised;
- Ensuring that risks have been considered appropriately and effective mitigations put in place;
- Providing an independent statement of why they believe a proposed operation is both necessary and proportionate;
- Setting and conducting meaningful Reviews;
- Cancelling authorisations when they are no longer necessary;
- Keeping notes regarding authorisations;
- Retaining a personal copy of the OSC Procedures and Guidance and/or relevant successor Guidance issued by the IPCO;
- Ensuring correct procedures are followed regarding Authorisations, Reviews, Renewals and Cancellations.
- Providing instructions regarding the management of any product to ensure it is managed appropriately with reference to the Council's RIPSA and Information/Records Management policies and procedures.
- Referring authorisation for the acquisition of confidential information or engagement of a vulnerable or juvenile CHIS to the Chief Executive (see Sections 8.11.3-8.12 below for further information.)

6.4. Senior Responsible Officer (SRO)

The Senior Responsible Officer is a nominated individual who is responsible for the Council's overall RIPSA compliance. In addition to the responsibilities held by all staff, the SRO must:

- Be a member of the Council's senior corporate team;

- Ensure Authorising Officers are competent to carry out their duties;

- Ensure high-level policies are fit for purpose;

- Ensure appropriate processes are in place;

- Pro-actively audit, and where necessary report errors;

- Engage with members and the regulator, the Investigatory Powers Commissioner's Office (IPCO);

- Implement action plans following IPCO inspections.

6.5. RIPSA Gatekeeper / Coordinating Officer

The Coordinating Officer (also known as 'Gatekeeper') is the central contact for advice and guidance regarding the Council's RIPSA compliance. In addition to the obligations held by all staff, the Coordinating Officer is responsible for:

- Ensuring a central store and register of RIPSA documentation is maintained;

- Ensuring relevant policies and procedures are in place and up-to-date;

- Performing first-line enquiry handling relating to RIPSA;

- Undertaking internal monitoring of compliance;

- Providing relevant training to staff.

6.6 Chief Executive

Certain surveillance activities are considered to carry a higher level of risk and require additional safeguards. Covert surveillance operations must be referred to the Chief Executive for authorisation when:

- Knowledge of confidential information is likely to be acquired. Confidential information is defined in the RIPSA context as:

    - Communications subject to legal privilege;
    - Communications between MPs and constituents relating to constituency matters;
    - Matters of medical and journalistic confidentiality.

- A vulnerable individual or juvenile (i.e. under the age of 18) is to be used as a Covert Human Intelligence Source (CHIS).

7. TYPES OF SURVEILLANCE

7.1. Overt Surveillance

Most of the surveillance carried out by East Lothian Council officers will be done overtly - there will be nothing secretive or hidden about it. One way of making surveillance overt is by telling the subject that it will happen.

Examples of this could be where the alleged perpetrator of a noise nuisance is warned (preferably in writing) that noise will be recorded if the noise continues, or where an entertainment licence is issued subject to conditions and the licensee is told that officers may visit without notice and/or without identifying themselves to the owner/proprietor to check that the conditions are being met.

Overt surveillance does not require authorisation under RIPSA.

7.2. Covert Surveillance

In order to be considered under RIPSA, surveillance must be covert, i.e. the target is unaware that it is taking place, and it must be 'necessary'. The surveillance may be considered necessary if is for the 'specified grounds' of:

a) Preventing or detecting crime or preventing disorder;

b) The interests of public safety; or

c) Protecting public health.

There are different forms that covert surveillance can take:

7.2.1. Directed Surveillance

Directed Surveillance operations require RIPSA authorisation. Directed Surveillance is covert, but not intrusive, and is undertaken:

- For the purposes of a specific investigation or a specific operation;

- In such a manner as is likely to result in the obtaining of private information about a person (whether or not one is specifically identified for the purposes of the investigation or operation);

- Otherwise than by way of an immediate response to events.

7.2.2. Covert Human Intelligence Sources (CHIS)

CHIS operations require RIPSA authorisation. A person is a CHIS if:

a) he or she establishes or maintains a personal or other relationship with a person for the **covert purpose** of facilitating the doing of anything falling within paragraph b) or c);

b) he or she **covertly uses** such a relationship to obtain information or to provide access to any information to another person; or

c) he or she **covertly discloses** information obtained by the use of such a relationship or as a consequence of the existence of such a relationship.

A relationship is established or maintained for a **covert purpose** if and only if it is conducted in a manner that is calculated to ensure that one or more of the parties to the relationship is unaware of the purpose.

A relationship is **used covertly**, and information obtained is **disclosed covertly**, if and only if the relationship is used or the information is 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.

A local authority may use a CHIS in two main ways:

- Council officers may themselves act as Sources by failing to disclose their true identity in order to obtain information;

- Council officers may cultivate a member of the public or employee of a business under investigation to provide them with information on a regular basis.

In both cases the person or persons being investigated are unaware that this is taking place. CHIS authorisation does not

apply in circumstances where members of the public volunteer information as part of their normal civic duties or contact numbers specifically set up to receive anonymous information, such as crimestoppers; nor do they become a CHIS if they are asked if they can provide additional information, e.g. details of the suspect's vehicle or the time that they leave for work. However, someone might become a CHIS as a result of a relationship with East Lothian Council that began in this way and authorisation must then be sought.

7.2.3. Intrusive Surveillance

Intrusive surveillance is not open to local authorities. East Lothian Council officers must not undertake intrusive surveillance.

Covert surveillance is intrusive if it is:

- Carried out in relation to anything taking place on 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.

The definition of intrusive surveillance is determined by the location of the surveillance, not the nature of the information obtained.

7.2.4. Non-RIPSA covert surveillance

Some surveillance activities are conducted covertly, but do not meet the criteria for Directed Surveillance, CHIS, or Intrusive Surveillance, and so RIPSA does not apply. This includes the collection of non-private information which is publicly or commercially available, although care must be taken when gathering information that is made available online or via social media (for more information on online/social media surveillance, refer to Section 9 below).

RIPSA also does not apply in relation to the Council's 'ordinary functions.' Ordinary functions are those which are undertaken by all authorities, such as employment and contractual arrangements, as opposed to 'core functions' which are specific public functions. The disciplining of an employee is considered an ordinary function, which is not within the scope of RIPSA.

7.2.5. Examples of different types of surveillance

Examples	Type of Surveillance
• Dog Warden on patrol; • Signposted CCTV.	**Overt**
• CCTV cameras providing general traffic information; • Noise monitoring that only records decibel levels; • Disciplinary investigation; • Officers conducting a single preliminary visit to identify a site of interest; • Regulatory or professional disclosures that are required by law.	**Covert, non-RIPSA**
• Officers follow an individual over a period of time to establish whether s/he is working while claiming benefits; • Officers use online information as part of a specific investigation to acquire private information about the movements and associations of a former offender; • Covert cameras are erected near (not within) a residence to identify the source of vandalism.	**Directed Surveillance (RIPSA)**
• Establishing and maintaining a relationship over Facebook using a false profile; • Test purchases where the officer or another individual will be establishing a relationship for a covert operation.	**CHIS (RIPSA)**
• Planting a listening device in a person's home or vehicle.	**Intrusive (not permitted)**

8. AUTHORISATION FOR DIRECTED SURVEILLANCE / CHIS

8.1. A correct and proper authorisation will provide officers with the legal authority to carry out covert surveillance, enable the collection of evidence, and reduce the possibility of a legal challenge on both the action and the admissibility of the evidence.

8.2. When is RIPSA authorisation needed?

In identifying circumstances where RIPSA authorisation is needed, Council officers must consider whether the proposed surveillance activities meet the tests for authorisation listed below. **These tests do not in themselves determine whether Applications for authorisation should be approved by the Authorising Officer** – they are simply set out here as an aid in determining whether RIPSA authorisation is likely to be required in relation to surveillance activities carried out by Council officers. Authorising Officers must also consider the fuller picture of proposed activities as set out in the Application in relation to the legislation and the Council's compliance framework before granting approval.

Activities which only partially meet the tests below for either Directed Surveillance or CHIS are unlikely to require authorisation, however when in doubt officers should consult with the Coordinating Officer / Gatekeeper.

8.2.1. 'Statutory' or 'specified grounds'

Where covert surveillance activities are **necessary** to the 'statutory grounds' listed in Section 7.2 above, this test for authorisation in relation to both Directed Surveillance and CHIS is met.[2]

8.2.2. Directed Surveillance - specific investigation

In relation to Directed Surveillance, where officers are conducting a **specific** investigation or operation, i.e. pre-planned surveillance of a specific person or group of people, this test for authorisation is met.

8.2.3. Directed Surveillance – private information

In relation to Directed Surveillance, where the surveillance activities are likely to obtain 'private information', this test for authorisation is met.

Private information may include personal data, such as names, telephone numbers and address details. Where such information is acquired by means of covert surveillance of a person having a

[2] While the statutory grounds for Directed Surveillance and CHIS are set out in different sections of RIPSA (Sections 6.3 and 7.3, respectively), they are framed in identical terms.

reasonable expectation of privacy, a directed surveillance authorisation is appropriate.

Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information. This is likely to be the case where that person has a reasonable expectation of privacy even though acting in public and where a record is being made by a public authority of that person's activities for future consideration or analysis.

Private life considerations are particularly likely to arise if several records are to be analysed together in order to establish, for example, a pattern of behaviour, or if one or more pieces of information (whether or not available in the public domain) are covertly (or in some cases overtly) obtained for the purpose of making a permanent record about a person or for subsequent data processing to generate further information.

8.2.4. Directed Surveillance – advance planning

In relation to Directed Surveillance, where officers are acting otherwise than in an immediate response to events, this test for authorisation is met.

8.2.5. CHIS – forming and/or maintaining a relationship

In relation to CHIS, where officers will be establishing or maintaining a covert relationship to gain information, this test for authorisation is met.

8.3. Authorisation to carry out Directed Surveillance and/or CHIS operations may only be given by the designated Authorising Officers, or by the Chief Executive in relation to the acquisition of confidential information or the engagement of juveniles or vulnerable individuals as sources (see Sections 8.11.3-8.12 below).

8.4. Authorising Officers must have appropriate seniority within the Council, as defined in Schedule 1 of the 2010 Order (as updated and amended from time to time). At the time of implementation of this version of the Policy, the relevant Council roles held by Authorising Officers shall be at the Service Manager level or above.

8.5. Applications, Reviews, Renewals and Cancellations must be in writing using the Council's standard Forms and templates for both Directed Surveillance and CHIS operations. These templates will form part

of the compliance framework and will capture all required information as set out within the Codes of Practice.

8.6. Investigating Officers are encouraged to consult with the Coordinating Officer / Gatekeeper prior to submitting an Application for authorisation.

8.7. Nominated Officers (as set out in Sections 6.2-6.6 above) shall operate at all times in a manner consistent with the Codes of Practice, any and all Guidance issued by the IPCO and internal guidance issued in support of this Policy.

8.8. In particular, when preparing, authorising and monitoring applications, conducting operations under RIPSA, and managing information obtained via such operations, the nominated Officers will have due regard for the following considerations:

8.8.1. Necessity

Directed surveillance / CHIS operations must be necessary on one or more statutory grounds (see Section 7.2 above).

8.8.2. Proportionality

If the surveillance / CHIS activities are deemed necessary on one or more statutory grounds, the person granting the authorisation must also believe that they are proportionate to what is sought to be achieved by carrying them out. This applies both to the authorisation of Directed Surveillance and the authorisation of the use and/or conduct of a CHIS. The consideration of proportionality involves balancing the seriousness of the intrusion into the privacy of the subject of the operation (or any other person who may be affected) against the need for the activity in investigative and operational terms.

The authorisation will not be proportionate if it is excessive in the overall circumstances of the case. Each action authorised should bring an expected benefit to the investigation or operation and should not be disproportionate or arbitrary. No activity should be considered proportionate if the information which is sought could reasonably be obtained by other less intrusive means (in the ordinary sense).

The following elements of proportionality should therefore be considered:

- balancing the size and scope of the proposed activity against the gravity and extent of the perceived crime or offence;

- explaining how and why the methods to be adopted will cause the least possible intrusion on the subject and others;

- considering whether the activity is an appropriate use of the legislation and having considered all reasonable alternatives, a reasonable way of obtaining the necessary result;

- evidencing, as far as is reasonably practicable, what other methods have been considered and why they were not implemented.

It is important therefore that all those involved in undertaking Directed Surveillance / CHIS activities or interference with property under RIPSA are fully aware of the extent and limits of the authorisation in question.

8.8.3. Collateral Intrusion

An application for authorisation should include an assessment of the risk of any collateral intrusion, i.e. the extent to which the surveillance will interfere with the privacy of persons other than the subject of the surveillance. Measures should be put in place to minimise unnecessary intrusion into privacy, which should be proportionate to the aim of the investigation. In relation to CHIS operations, the Authorising Officer should take this into account when considering the proportionality of the use and conduct of a source.

8.9. CHIS authorisations: additional considerations

8.9.1. An authorisation may be obtained under RIPSA for the **use** or **conduct** of a CHIS:

- The **use** of a CHIS involves any action on behalf of a public authority to induce, ask or assist a person to engage in the conduct of a CHIS. In general, therefore, an authorisation for use of a CHIS will be necessary to authorise steps taken by the Council in relation to a CHIS.

- The **conduct** of a CHIS is any conduct of a CHIS which falls within section 7.2.2(a) to (c) above or is incidental to anything falling within that section. In other words, an authorisation for conduct will authorise steps taken by the CHIS on behalf, or at the request, of the Council.

8.9.2. Care must be taken to ensure that the CHIS is clear on what is/is not authorised at any given time and that all the CHIS's activities are properly risk assessed. Care should also be taken to ensure that relevant Applications, Reviews, Renewals and Cancellations are correctly performed and recorded in line with the Codes of Practice. A CHIS may in certain circumstances be the subject of different use or conduct authorisations obtained by one or more public authorities. Such authorisations should not conflict.

8.9.3. Nominated Officers as listed in Sections 6.2-6.6 above must ensure that all **use** or **conduct** is:

- necessary and proportionate to the intelligence dividend that it seeks to achieve; and

- in compliance with relevant Articles of the European Convention on Human Rights (ECHR), particularly Articles 6 (right to a fair trial) and 8 (right to respect for private and family life).

8.9.4. Authorisation is required where a relationship exists between the subject and the CHIS, even if specific information is not being sought by the Council. Unlike Directed Surveillance (which relates specifically to private information), authorisations for the use or conduct of a CHIS do not relate specifically to private information, but to the covert forming and/or maintaining of a relationship to gain any information.

8.9.5. The Council's nominated Officers listed in Sections 6.2-6.6 above will ensure that arrangements are in place for the proper oversight and management of CHIS, including appointing individual officers as defined in Section 7(6)(a) of RIPSA for each CHIS. The person referred to in Section 7(6)(a) of the 2000 Act, the "handler", will have day to day responsibility for:

- dealing with the CHIS on behalf of the authority concerned;
- directing the day to day activities of the CHIS;
- recording the information supplied by the CHIS; and
- monitoring the CHIS's security and welfare.

The handler of a CHIS will usually be of rank or position below that of the Authorising Officer.

8.9.6. The Council templates for Authorisation, Review, Renewal, and Cancellation of operations, as well as records in relation to individual Sources, shall capture all relevant information as

required by RIPSA legislation (as updated and amended from time to time) and as recommended in the Codes of Practice.

8.9.7. In deploying a Source, the Authorising Officer must take into account the safety and welfare of that source when carrying out actions in relation to an authorisation or tasking, and to foreseeable consequences to others of that tasking. Before authorising the use or conduct of a source, the Authorising Officer should ensure that a **risk assessment** is carried out to determine the risk to the source of any tasking and the likely consequences should the role of the Source become known. The ongoing security and welfare of the Source, after the cancellation of the authorisation, should also be considered at the outset.

8.9.8. The same provisions for the Review, Renewal and Cancellation of CHIS authorisations apply as for Directed Surveillance (noting the differences regarding duration as set out in Section 8.11 below). Additionally, the ongoing safety and welfare of the Source should continue to be taken into account, even after the authorisation has been cancelled.

8.10. **Urgent authorisations**

8.10.1. Urgent authorisations should not normally be necessary. In exceptional circumstances, however, urgent authorisations may be given orally if the time that would elapse before a written authorisation can be granted would either be likely to (1) endanger life or (2) jeopardise the investigation or operation for which the authorisation was being given. Urgent authorisations will normally only be given following consultation with the SRO or the Chief Executive.

8.10.2. An application will never be urgent where the need for authorisation has been neglected or is of the Applicant's own making.

8.10.3. Where authorisations are granted orally under urgency procedures, a record detailing the actions authorised and the reasons why the urgency procedures were used should be recorded by the Applicant and Authorising Officer as a priority.

8.11. **Duration of authorisations**

Authorisations must be granted in line with the following timescales, and not for shorter initial durations than those listed below. They must be formally cancelled at the end of the authorisation period

using the relevant template. **Authorisations must not be allowed to expire.**

8.11.1. Directed Surveillance

A written authorisation for Directed Surveillance will cease to have effect (unless renewed or cancelled) at the end of a period of **three months** beginning with the day when the authorisation granted has taken effect.

Urgent oral authorisations or written authorisations granted by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after **72 hours**, beginning with the time when the authorisation granted had taken effect.

8.11.2. CHIS

A written authorisation will, unless renewed or cancelled, cease to have effect at the end of a period of **12 months** beginning with the day on which it took effect, except in the case of juvenile CHIS or in the case of matters pertaining to the 2014 Order.

Urgent oral authorisations or authorisations granted or renewed by a person who is entitled to act only in urgent cases will, unless renewed, cease to have effect after **72 hours**, beginning with the time when the authorisation was granted.

Authorisations may be renewed for a further period of **12 months**.

8.11.3. CHIS – Vulnerable / Juvenile Sources

Authorisations for vulnerable or juvenile Sources should be granted **only by the Chief Executive**. The duration of such an authorisation is **one month** from the time of grant or renewal (instead of 12 months). For these purposes, the age test is applied at the time of the grant or renewal of the authorisation.

8.12. **Special considerations: confidential information, juveniles and vulnerable individuals**

Any Directed Surveillance operations that capture confidential information or involve the engagement of a vulnerable individual or juvenile as a CHIS **must be authorised by the Chief Executive**, or in their absence a nominated Executive Director deputising on their behalf.

8.12.1. 'Confidential information' includes:

- Communications subject to legal privilege;
- Communications between MPs and constituents relating to constituency matters;
- Matters of medical and journalistic confidentiality.

8.12.2. A 'juvenile source' is a person under the age of 18. On no occasion should the use or conduct of a CHIS under 16 years of age be authorised to give 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; SSI No. 206 are satisfied.

8.12.3. 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 and who is or may be unable to take care of him/herself, or unable to protect him/herself against significant harm or exploitation. Any individual of this description should only be authorised to act as a CHIS in the most exceptional circumstances.

9. ONLINE AND SOCIAL MEDIA SURVEILLANCE

9.1. Council Officers may be called upon in the course of their duties to undertake surveillance by accessing websites or social media content. The above provisions apply equally to such activities as to offline / in person operations. It is therefore important for officers to understand when online or social media activities call for RIPSA authorisation.

9.2. Surveillance activities needing authorisation might include:

- Visiting a third-party website or accessing social media posts, profiles or groups only once;

- Visiting/viewing websites, posts, profiles and/or groups regularly over a period of time;

- Entering into a personal relationship with a third party or parties via online or social media platforms.

9.3. Where online research or investigation is conducted covertly for the purpose of a specific investigation or operation and is likely to result in the obtaining of private information about a person or group, an authorisation for Directed Surveillance should be considered. Where

a person acting on behalf of a public authority is intending to engage with others online without disclosing his or her identity, a CHIS authorisation may be needed.

9.4. In deciding whether online surveillance should be regarded as covert, consideration should be given to the likelihood of the subject(s) knowing that the surveillance is or may be taking place. Use of the internet itself may be considered as adopting a surveillance technique calculated to ensure that the subject is unaware of it, even if no further steps are taken to conceal the activity. Conversely, if reasonable steps have been taken to inform the public or particular individuals that the surveillance is or may be taking place this can be regarded as overt and a directed surveillance authorisation will not normally be available.

9.5. While individuals may have a reduced expectation of privacy in relation to information that is made generally and publicly available by the individual online or on social media, information posted on personal social networking sites which are normally accessed by a smaller circle of personal contacts is likely to include private information to which an expectation of privacy would apply and fall within the scope of a person's private life. Whether the Council interferes with a person's private life includes a consideration of the nature of the Council's activity in relation to that information. This is regardless of whether or not the account holder has applied any privacy settings to the account.

9.6. Factors that should be considered in establishing whether a Directed Surveillance authorisation is required include whether:

- the investigation or research is directed towards an individual or group of people;
- it is likely to result in obtaining private information about a person or group of people;
- it is likely to involve building up an intelligence picture or profile;
- the information obtained will be recorded and stored;
- the information is likely to provide an observer with a pattern of lifestyle;
- the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;

- the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);

- it is 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.

9.7. Regarding CHIS, where a website or social media account requires a minimal level of interaction (such as sending or receiving a friend request before access is permitted) this may not in itself amount to establishing a relationship. Equally, the use of electronic gestures such as "like" or "follow" in order to react to information posted by others online would not in itself constitute forming a relationship. However, it should be borne in mind that entering a website or responding on these gestures may lead to further interaction with other users. A CHIS authorisation should be obtained if it is intended to engage in such interaction to obtain, provide access to or disclose information.

9.8. In relation to online and social media surveillance, Council officers should refer to the above guidance regarding Directed Surveillance and CHIS activities and refer any questions to the Council's Coordinating Officer / Gatekeeper. If authorisation is required, all relevant procedural steps for the type of surveillance should be followed, with reference to the Council's supporting compliance framework.

9.9. <u>Provisions for surveillance using online platforms/social media:</u>

9.9.1. Council officers must not use their own private accounts to view the accounts/profiles of other individuals for an investigation under any circumstances. If, in their personal time, officers using their private accounts encounter information based on personal connections, they cannot use this information for the purposes of an investigation. Rather, an official investigation will have to be initiated and, where necessary, the proper authorisations under RIPSA must be obtained.

9.9.2. Officers using a specially created departmental identity in order to 'friend' individuals with closed, privacy-protected profiles on social networks will require a CHIS authorisation granted and approved by an Authorising Officer.

9.9.3. Officers instructing a third party using their own private identity to conduct an investigation on a person they are connected with through social media will require a CHIS authorisation granted and approved by an Authorising Officer.

10. RECORDS MANAGEMENT

10.1. A central record of all Authorisations, Reviews, Renewals, Cancellations and Rejections will be maintained and monitored by the Coordinating Officer / Gatekeeper. Each Form will have a unique reference number (URN). The cross-referencing of each URN takes place within the Forms for audit purposes. Rejected Forms will also have URNs.

10.2. In addition to the central record, the Coordinating Officer / Gatekeeper will manage and maintain the following records in relation to each Authorisation:

- Copies of the Application, Review, Renewal and Cancellation Forms (as relevant) together with any supplementary documentation;
- Copies of any Risk Assessments carried out prior to authorisation;
- Notification of the approval given by the Authorising Officer;
- A record of the period over which the operation has taken place;
- The frequency of reviews prescribed by the Authorising Officer;
- A record of the result of each review of the Authorisation;
- The date(s) and time(s) of any instructions issued by the Authorising Officer.

It is likely that the Coordinating Officer / Gatekeeper will not have routine access to the records listed above in the course of the activities of the operation. The Investigating Officer and Authorising Officer must therefore ensure that all relevant records are passed to the Coordinating Officer / Gatekeeper for central management and storage.

10.3. The record copy held by the Coordinating Officer / Gatekeeper is considered the 'golden copy', i.e. the official and most complete version of the record. A robust audit trail must be maintained regarding the creation, management and disposition of this record in line with the Council's Information and Records Management Policy, and all other copies should be destroyed as soon as they are no longer required for immediate business. No copy should be retained for a longer period than the golden copy.

10.4. All RIPSA-related Forms and documentation, including risk assessments, will be securely stored in digital format, and should be made available to the IPC or his/her Inspector upon request.

10.5. Record retention

10.5.1. Records must be retained to allow the Investigatory Powers Tribunal (IPT) to carry out its functions. The IPT will consider complaints made up to one year after the conduct to which the complaint relates and, where it is equitable to do so, may consider complaints made more than one year after the conduct to which the complaint relates (see section 67(5) of RIPA), particularly where continuing conduct is alleged.

10.5.2. The standard retention period for RIPSA Forms and associated records shall therefore be **5 years**, unless other requirements imposed by criminal or civil proceedings, other legal and/or regulatory regimes, or other matters of pressing concern take exceptional precedence.

10.5.3. Any decision to modify this retention period in relation to individual records shall be documented and authorised by the Senior Responsible Officer with reference to the Council's Records Management policies and procedures. Provision for RIPSA Forms and RIPSA-related records shall be included in the Council's corporate Retention Schedule.

10.6. All RIPSA-related records must be maintained in line with the Council's Information and Records Management Policy, Records Management Plan, Data Protection Policy and IT Acceptable Use Policy.

10.7. RIPSA-related records should never be stored or sent outwith the Council environment, including the Council's digital network controls, unless the records are being securely transferred for a legitimate purpose, e.g. the provision of records to the IPC or his/her Inspector. In relation to the sharing of records, the Council's most up-to-date Information Security recommendations and the provisions of any relevant Data Sharing Agreements must be followed.

10.8. Management of product (covert material)

10.8.1. The management of product, i.e. information acquired as a result of RIPSA operations, is the responsibility of the Investigating Officer (**not** the Coordinating Officer / Gatekeeper). The Investigating Officer must ensure that product is managed in line

with the Authorising Officer's instructions and with reference to this Policy and the Council's information/records management policies and procedures. With the exception of this point regarding responsibility for its management, the same Records Management provisions apply to product as to other RIPSA-related documentation.

10.8.2. Product (i.e. records) can appear in many different formats, including audio/video recording, paper documentation, email, and more. The same records management provisions apply to these formats and materials as to other Council records and information.

10.8.3. 'Data pathways' should be identified for all covert material acquired via RIPSA operations, e.g. via the Council's Information Asset Register. Every effort should be made to reduce duplication as much as possible.

10.8.4. When covert material is formally handed over from one team to another, clear instructions should be given to the recipient so they understand expectations for handling such material and who holds responsibility for its onward management.

10.8.5. The use of removable media should be avoided. If it cannot be avoided, advice should be sought from the Council's Information Security specialists regarding the use of sufficiently secure methods of transferring and/or transporting the information.

10.8.6. The product held by the Investigating Officer is the 'golden copy' record, and all associated provisions apply (see Section 10.3 above). The Investigating Officer should ensure that s/he holds and maintains the most complete and authoritative version of the material.

10.8.7. Product must be retained within an agreed File Plan using consistent file naming conventions, with reference to the Council's corporate File Planning and File Naming guidance.

10.8.8. Covert material (product) should be retained no longer than is necessary, with a robust audit trail maintained for the creation, storage, sharing, destruction or other permanent transfer of the material.

10.8.9. Any questions or uncertainties regarding the management of product or other records should be referred to the Council's Coordinating Officer / Gatekeeper and Team Manager-Information

Governance (or other relevant officer tasked with monitoring and facilitating information and records management compliance).

11. TRAINING

11.1. All Authorising and Investigating Officers are required to undergo regularly refreshed training provided by the Coordinating Officer / Gatekeeper to ensure compliance with the requirements of the law.

11.2. All staff shall undertake role-relevant training regarding the content of this Policy, the compliance framework, and the requirements of the law.

12. INVESTIGATORY POWERS COMMISSIONER

12.1. The office of the Investigatory Powers Commissioner (IPCO) has responsibility for overseeing the procedures employed by all authorities engaged in covert surveillance. Part of its role is to periodically examine and audit the records and procedures of authorities, and the Council's Authorisation Officers must be prepared to justify their actions when called upon to do so.

13. COMPLAINTS

13.1. Any person who reasonably believes that they have been adversely affected by any activities carried out pursuant to this Policy by or on behalf of the Council may complain to the Senior Responsible Officer who will investigate the complaint. Such a person may also complain to the Investigatory Powers Tribunal:

By post: Investigatory Powers Tribunal
PO Box 33220
London
SWlH 9ZQ

By email: info@ipt-uk.com

14. REVIEW AND OVERSIGHT

Elected members shall review the Council's use of RIPSA and compliance with the Policy once a year.

In circumstances where it is justified by the volume of applications authorised and/or rejected, internal reports on the use of RIPSA shall be made to elected members on a quarterly basis to ensure that it authorisations are being used consistently with this Policy and that the Policy remains fit for purpose.

Reporting to elected members shall be for the purposes of overall accountability and oversight of RIPSA activities in relation to this Policy. Elected members shall not, however, be involved in making decisions on specific authorisations.

The Policy shall be formally reviewed and re-submitted to Elected Members for approval every three years.