

North Lanarkshire Council Report

Policy and Strategy Committee

Does this report require to be approved? Yes No

Ref REB/CC

Date 11/06/26

Governance, Oversight and Compliance Arrangements under the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA)

From Rachel Blair, Chief Officer (Legal, Democratic and Strategy)

E-mail BlairR@northlan.gov.uk

Executive Summary

This report provides the Policy and Strategy Committee with a comprehensive update on the Council's governance, compliance, and assurance arrangements in relation to the Regulation of Investigatory Powers (Scotland) Act 2000 (RIPSA). This legislative framework regulates the lawful use of covert investigatory techniques by public authorities, including directed surveillance, the use of covert human intelligence sources (CHIS), and certain forms of communications data acquisition.

The use of covert investigatory powers represents one of the most intrusive functions exercised by a public authority and therefore requires a robust framework of legal compliance, operational governance, oversight, accountability, and democratic assurance. RIPSA establishes clear statutory safeguards designed to ensure that any interference with an individual's right to privacy under Article 8 of the European Convention on Human Rights (ECHR) is lawful, necessary, proportionate, properly authorised, and subject to appropriate scrutiny.

Failure to comply with RIPSA and associated Codes of Practice may expose the Council to significant legal, financial, operational, and reputational risks, including judicial challenge, evidential inadmissibility, criticism from the Investigatory Powers Commissioner's Office (IPCO), regulatory intervention, and potential findings of unlawful interference with Convention rights.

The report outlines the Council's current compliance position following engagement with IPCO as part of the 2026 inspection cycle. It confirms that IPCO reviewed the Council's written compliance submission and determined that no further inspection activity or follow-up engagement was required at this stage. This provides significant external assurance regarding the effectiveness of the Council's current governance and compliance arrangements.

The report also sets out a programme of continuous improvement designed to strengthen operational practice, governance arrangements, training, oversight, and organisational awareness. This includes:

- revision and annual review of the RIPSA Policy;
- strengthened authorisation and cancellation processes;
- enhanced guidance relating to social media and online investigations;
- establishment of quarterly and annual reporting arrangements to elected members;

- delivery of mandatory and refresher training;
- quality assurance reviews of applications and authorisations; and
- revised governance arrangements for Authorising Officers to ensure consistency, competence, and operational resilience.

In addition, the report proposes that the RIPSAs Policy and associated governance arrangements be incorporated within the Council's wider Strategic Governance Framework review programme. This would recognise RIPSAs compliance as an important component of the Council's corporate governance architecture and would enable reference to the existence and operation of the RIPSAs Policy within the Council's Annual Governance Statement. This approach would further strengthen organisational assurance, transparency, and elected member oversight through existing governance reporting mechanisms, including reporting to the Audit and Scrutiny Panel.

The report therefore reflects not only operational compliance with investigatory powers legislation, but also the Council's wider commitment to lawful decision-making, ethical governance, accountability, transparency, and the protection of individual rights.

Recommendations

It is recommended that Policy and Strategy Committee:

- (1) Acknowledges the response submitted to the Investigatory Powers Commissioner's Office (IPCO) outlining the Council's compliance arrangements and notes that no further inspection activity or follow-up engagement has been required at this stage;
- (2) Acknowledges the Council's strong overall compliance position and the constructive feedback provided by IPCO in relation to opportunities for continuous improvement;
- (3) Acknowledges the revised governance arrangements for RIPSAs compliance, including the introduction of a smaller and operationally focused group of Authorising Officers to strengthen consistency, oversight, and decision-making quality;
- (4) Approves the updated RIPSAs Policy attached at Appendix 1;
- (5) Approves the proposed Social Media and Online Investigative Activity Monitoring Form attached at Appendix 2;
- (6) Acknowledges the ongoing programme of improvement and compliance activity, including:
 - i. annual review of the RIPSAs Policy;
 - ii. quarterly governance reporting arrangements and formal annual assurance reporting to elected members;
 - iii. strengthened quality assurance and audit arrangements;
 - iv. mandatory and refresher training for relevant officers;
 - v. enhanced application and authorisation templates;
 - vi. strengthened cancellation and review processes; and
 - vii. improved oversight of social media and online investigative activity;
- (7) Approves the introduction of a formal annual reporting arrangement to the Policy and Strategy Committee on the Council's use of investigatory powers under the Regulation of Investigatory Powers (Scotland) Act 2000, including information relating to governance, compliance activity, training, authorisations, oversight arrangements, audit findings, and continuous improvement actions, in order to support ongoing democratic oversight, transparency, accountability, and governance assurance;
- (8) Approve the incorporation of the Council's RIPSAs Policy and associated compliance arrangements within the Strategic Governance Framework review programme and acknowledge that reference to these arrangements will be included within the

- Council's Annual Governance Statement as part of the Council's wider governance assurance framework; and
- (9) Acknowledges the continuing role of the Chief Officer (Legal, Democratic and Strategy), as Senior Responsible Officer, in maintaining oversight of compliance, governance, assurance, and organisational accountability in relation to investigatory powers legislation.
-

The Plan for North Lanarkshire

Priority	All priorities
Ambition statement	All ambition statements
Programme of Work	Statutory / corporate / service requirement

1. Background

- 1.1 The Regulation of Investigatory Powers (Scotland) Act 2000 ("RIPSA") and the Investigatory Powers Act 2016 ("IPA") establish the statutory framework governing the use of certain covert investigatory techniques by public authorities, including local authorities. These powers are primarily utilised in connection with regulatory, enforcement, investigatory and public protection functions and are subject to strict legal safeguards, oversight and authorisation requirements.
- 1.2 The legislation governs activities including directed surveillance, the use of covert human intelligence sources ("CHIS"), and the acquisition of communications data. Any use of these powers must satisfy statutory tests of legality, necessity and proportionality and must be authorised by appropriately trained officers acting under delegated authority.
- 1.3 The lawful use of covert investigatory powers is an area of significant legal, operational and reputational importance. RIPSA plays a critical role in safeguarding individuals' rights under Article 8 of the European Convention on Human Rights ("ECHR"), which protects the right to respect for private and family life. Failure to comply with the statutory framework may result in legal challenge, reputational damage, regulatory criticism, exclusion of evidence in proceedings, or findings of unlawful interference with privacy rights.
- 1.4 Oversight and accountability are provided through the Investigatory Powers Commissioner's Office ("IPCO"), which conducts inspections and compliance reviews of public authorities to assess governance arrangements, operational compliance, quality of authorisations, training, record keeping, and organisational awareness.
- 1.5 The Council was scheduled for its next three-yearly inspection cycle during 2026. As part of the revised inspection approach, IPCO requested the submission of written assurance documentation outlining the Council's current compliance arrangements and governance framework. The Council submitted the required response within the prescribed timescale. The feedback received from IPCO was constructive and confirmed that the Council's overall compliance arrangements remain strong. IPCO identified a number of areas operating effectively together with opportunities for further strengthening and continuous improvement, particularly in relation to:
- articulation of necessity and proportionality within applications and authorisations;
 - differentiation between background narrative and operational justification;
 - oversight of social media investigative activity;

- consistency of cancellation processes; and
 - enhanced elected member oversight arrangements.
- 1.6 The Senior Responsible Officer (“SRO”) for RIPSAs within the Council is the Chief Officer (Legal, Democratic and Strategy), who has overall responsibility for oversight of the Council’s compliance arrangements, governance framework and assurance mechanisms. The Council’s Authorising Officer arrangements have been revised to provide a smaller, operationally focused cohort of appropriately trained officers in line with IPCO expectations and governance best practice. The revised Authorising Officers are:
- Chief Officer (Audit and Risk);
 - Chief Officer (Community Operations);
 - Chief Officer (Legal, Democratic and Strategy); and
 - Business Manager (Regulatory Services).
- 1.7 There remains an ongoing operational requirement to ensure that all relevant officers maintain appropriate awareness and understanding of RIPSAs requirements, Codes of Practice, and associated governance obligations. Training was delivered during March 2026 for Authorising Officers, applying officers, Legal and Democratic staff, and relevant operational services.
-

2. Report

Current Use of Covert Powers

- 2.1 Since the last IPCO inspection in 2023, covert investigatory powers have been utilised by the Protective Services Team in relation to directed surveillance activity. Nineteen directed surveillance authorisations have been granted during this period. There has been no use of Covert Human Intelligence Source (“CHIS”) powers since the previous inspection cycle.
- 2.2 The Council maintains comprehensive electronic records and central registers relating to all RIPSAs activity, including:
- central registers of authorisations;
 - application and authorisation documentation;
 - review and cancellation records; and
 - CHIS records where applicable.

Updated RIPSAs Policy

- 2.3 A revised RIPSAs Policy has been prepared to reflect current legislation, statutory Codes of Practice, operational guidance, governance expectations and emerging investigative practice. The revised policy includes:
- expanded guidance and operational examples relating to directed surveillance;
 - updated guidance on necessity and proportionality assessments;
 - strengthened provisions relating to collateral intrusion;
 - revised guidance on confidential material and retention;
 - a new dedicated section relating to social media and online investigations;
 - updated guidance relating to communications data; and
 - clarification of governance, oversight and authorisation responsibilities.

2.4 The policy also reflects the expectation that public authorities maintain robust governance arrangements, regular policy review mechanisms, and clear operational guidance capable of evidencing compliance during regulatory inspection activity. The RIPSA Policy will now be subject to annual review by the Information Governance Team to ensure continued compliance with legislation, statutory Codes of Practice, IPCO expectations and technological developments.

Social Media and Online Investigations

2.5 The increasing use of social media and online investigative techniques creates additional governance and compliance considerations for local authorities undertaking investigatory or enforcement activity. The updated policy therefore includes a dedicated section relating to online investigative activity and social media surveillance. The revised guidance distinguishes between:

- ad hoc viewing of publicly available content;
- repeated or systematic monitoring amounting to directed surveillance; and
- covert interaction or relationship building amounting to CHIS activity.

2.6 The guidance also reinforces that:

- officers must never use personal social media accounts for investigative activity;
- all investigative activity must be necessary and proportionate;
- authorisation routes must be followed where required; and
- all activity must be appropriately recorded and capable of audit scrutiny.

2.7 To strengthen governance and oversight arrangements, a dedicated monitoring form for online and social media investigative activity has been developed. This will support:

- auditability;
- regulatory assurance;
- oversight of cumulative activity;
- early identification of authorisation requirements; and
- evidence of compliance during future IPCO inspections.

Governance, Oversight and Assurance Framework

2.8 In addition to the operational and compliance measures outlined in this report, consideration has been given to strengthening the Council's wider corporate governance assurance arrangements in relation to RIPSA.

2.9 It is proposed that the Council's RIPSA Policy, associated governance arrangements, oversight mechanisms, training framework and elected member reporting arrangements are incorporated within the Council's Strategic Governance Framework review programme as a recognised governance mechanism and source of assurance.

2.10 The Strategic Governance Framework provides the overarching structure through which the Council identifies, reviews and evidences the governance arrangements, controls, policies and assurance mechanisms that support effective governance, accountability, legal compliance and risk management across the organisation.

2.11 Incorporating RIPSA within that framework will:

- provide a clearer corporate governance record of the Council's investigatory powers arrangements;
 - strengthen organisational assurance regarding compliance with statutory investigatory powers legislation;
 - support transparency and accountability in relation to covert surveillance activity;
 - ensure RIPSAs are considered as part of wider governance assurance reviews; and
 - support future internal audit, external audit and IPCO inspection activity.
- 2.12 It is also proposed that reference to the Council's RIPSAs Policy and governance arrangements be included within the Council's Annual Governance Statement moving forward. This will provide additional assurance to the Audit and Scrutiny Panel and demonstrate that appropriate governance mechanisms are in place to support lawful and proportionate use of investigatory powers.
- 2.13 The Strategic Governance Framework and Annual Governance Statement are both reported annually to the Audit and Scrutiny Panel, thereby ensuring continued visibility, oversight and governance assurance in relation to RIPSAs compliance arrangements.

Elected Member Oversight and Reporting

- 2.14 While RIPSAs do not expressly mandate quarterly reporting to elected members, IPCO expects local authorities to maintain effective democratic oversight arrangements in relation to covert surveillance activity. Quarterly reporting arrangements will therefore be introduced to provide elected members with statistical and governance information relating to:
- numbers and types of authorisations;
 - refusals, renewals and cancellations;
 - service areas involved;
 - training activity;
 - governance issues identified; and
 - compliance monitoring outcomes.
- 2.15 These arrangements will support transparency, accountability and assurance while ensuring that elected members are appropriately informed regarding the Council's use of covert powers.
- 2.16 In addition to quarterly governance reporting arrangements, an annual assurance report on the Council's use of investigatory powers and associated compliance framework will be presented to the Policy and Strategy Committee to support continued democratic oversight, transparency, governance assurance, and organisational accountability.

Training and Continuous Improvement

- 2.17 Interactive RIPSAs training sessions were delivered during March 2026 by a specialist RIPSAs practitioner. Attendance included the Chief Executive, Authorising Officers, applying officers and operational officers whose roles require awareness of RIPSAs.
- 2.18 A programme of continuous improvement has been developed which includes:
- mandatory training requirements;
 - annual refresher sessions;

- maintenance of a central training register;
- quality assurance review of applications and authorisations;
- strengthening of application templates;
- review of cancellation processes; and
- ongoing communication of legal and operational developments.

Conclusion

- 2.19 The lawful use of covert investigatory powers is an area of significant legal, operational and reputational importance for all public authorities. The Regulation of Investigatory Powers (Scotland) Act 2000 and the Investigatory Powers Act 2016 provide an essential statutory framework designed to balance the legitimate investigatory functions of local authorities with the protection of individual rights and freedoms under Article 8 of the European Convention on Human Rights.
- 2.20 The Council's current arrangements demonstrate a strong level of compliance and governance maturity, supported by trained Authorising Officers, established oversight arrangements, clear record management processes, effective engagement with IPCO, and a commitment to continuous improvement.
- 2.21 The improvement actions outlined within this report will further strengthen the Council's governance framework through enhanced oversight, clearer operational guidance, strengthened social media controls, structured training programmes, regular elected member reporting, and integration within the Council's wider Strategic Governance Framework.
- 2.22 Collectively, these arrangements will support continued lawful, proportionate and accountable use of investigatory powers while ensuring that the Council remains well placed to respond to future regulatory expectations, technological developments, and evolving investigatory practice.

3. Measures of success

- 3.1 The success of the revised governance and compliance arrangements will be measured against the following criteria:
- 3.1.1 Continued compliance with the requirements of the Regulation of Investigatory Powers (Scotland) Act 2000, the Investigatory Powers Act 2016, and associated statutory Codes of Practice;
 - 3.1.2 Positive assurance outcomes from IPCO inspections, engagement activity, and any future regulatory review;
 - 3.1.3 Maintenance of up-to-date policies, procedures, governance arrangements and operational guidance;
 - 3.1.4 Effective delivery and completion of mandatory and refresher training for relevant officers
 - 3.1.5 Improved quality, consistency and robustness of RIPSAs applications, authorisations, reviews and cancellations;
 - 3.1.6 Effective monitoring and governance oversight of social media and online investigative activity;
 - 3.1.7 Implementation of quarterly and annual elected member reporting arrangements;

- 3.1.8 Integration of RIPSAs governance arrangements within the Strategic Governance Framework and Annual Governance Statement assurance process; and
 - 3.1.9 Continued assurance that investigatory powers are only utilised where lawful, necessary, proportionate and operationally justified.
-

4. Supporting documentation

- 4.1 Appendix 1 - RIPSAs Policy
- 4.2 Appendix 2 - Online/Social Media Investigations Form
- 4.3 Appendix 3 - IPCO – Response to Compliance Inspection Request
- 4.4 Appendix 4 - IPCO Investigation Outcome Letter



Name Rachel Blair
Title Chief Officer (Legal, Democratic and Strategy)

5. Impacts

<p>5.1 Public Sector Equality Duty and Fairer Scotland Duty Does the report contain information that has an impact as a result of the Public Sector Equality Duty and/or Fairer Scotland Duty? Yes <input type="checkbox"/> No <input checked="" type="checkbox"/> If Yes, please provide a brief summary of the impact?</p> <p>If Yes, has an assessment been carried out and published on the council's website? https://www.northlanarkshire.gov.uk/your-community/equalities/equality-and-fairer-scotland-duty-impact-assessments Yes <input type="checkbox"/> No <input type="checkbox"/></p>
<p>5.2 Financial impact Does the report contain any financial impacts? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If Yes, have all relevant financial impacts been discussed and agreed with Finance? Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact? The report has limited direct financial implications associated with the delivery of training, policy review, governance oversight, compliance monitoring, and ongoing administration of RIPSAs arrangements. These activities will be managed within existing service resources and budgets. Effective governance and compliance arrangements also assist in mitigating potential financial risks associated with unlawful surveillance activity, litigation, regulatory criticism, compensation claims, or reputational damage.</p>
<p>5.3 HR policy impact Does the report contain any HR policy or procedure impacts? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If Yes, have all relevant HR impacts been discussed and agreed with People Resources? Yes <input type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact? The report includes requirements relating to staff awareness, mandatory training, refresher training, operational guidance, and governance responsibilities for officers involved in investigatory activity. The revised arrangements support staff competency, consistency of practice, and compliance with statutory and professional obligations.</p>
<p>5.4 Legal impact Does the report contain any legal impacts (such as general legal matters, statutory considerations (including employment law considerations), or new legislation)? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If Yes, have all relevant legal impacts been discussed and agreed with Legal and Democratic? Yes <input checked="" type="checkbox"/> No <input type="checkbox"/> If Yes, please provide a brief summary of the impact? The report relates directly to the Council's statutory obligations under the Regulation of Investigatory Powers (Scotland) Act 2000, the Investigatory Powers Act 2016, associated Codes of Practice, and obligations arising under Article 8 of the European Convention on Human Rights. The report sets out the Council's governance, oversight, authorisation, training and compliance arrangements designed to ensure</p>

that covert investigatory activity is undertaken lawfully, proportionately and in accordance with statutory requirements.

The updated RIPSAs Policy, strengthened governance arrangements, revised Authorising Officer structure, and enhanced monitoring processes are intended to mitigate legal risk, support compliance assurance, and ensure that investigatory activity is capable of withstanding legal and regulatory scrutiny.

5.5 Data protection impact

Does the report / project / practice contain or involve the processing of personal data?

Yes No

If Yes, is the processing of this personal data likely to result in a high risk to the data subject?

Yes No

If Yes, has a Data Protection Impact Assessment (DPIA) been carried out and e-mailed to dataprotection@northlan.gov.uk

Yes No

5.6 Technology / Digital impact

Does the report contain information that has an impact on either technology, digital transformation, service redesign / business change processes, data management, or connectivity / broadband / Wi-Fi?

Yes No

If Yes, please provide a brief summary of the impact?

The report includes updated governance arrangements relating to digital investigatory activity, including the use of social media and online surveillance techniques. The revised policy and monitoring arrangements strengthen oversight of digital investigative practices and improve governance, auditability, and record management associated with online investigations.

The report also supports improvements to governance processes, compliance monitoring, electronic record management, and organisational assurance mechanisms linked to investigatory activity.

Where the impact identifies a requirement for significant technology change, has an assessment been carried out (or is scheduled to be carried out) by the Enterprise Architecture Governance Group (EAGG)?

Yes No

5.7 Environmental / Carbon impact

Does the report / project / practice contain information that has an impact on any environmental or carbon matters?

Yes No

If Yes, please provide a brief summary of the impact?

5.8 Communications impact

Does the report contain any information that has an impact on the council's communications activities?

Yes No

If Yes, please provide a brief summary of the impact?

The report includes proposals for ongoing communication, awareness raising, training and dissemination of guidance relating to RIPSAs obligations and investigatory powers governance arrangements. There will also be communication with relevant officers and services regarding updated policies, operational procedures, training requirements, and governance expectations.

5.9 Risk impact

Is there a risk impact?

Yes No

If Yes, please provide a brief summary of the key risks and potential impacts, highlighting where the risk(s) are assessed and recorded (e.g. Corporate or Service or Project Risk Registers), and how they are managed?

The use of covert investigatory powers carries significant legal, operational, governance and reputational risks if not exercised lawfully and appropriately. Risks include unlawful interference with privacy rights, non-compliance with statutory requirements, regulatory criticism, evidential challenges, reputational damage, and potential financial liability arising from complaints, litigation or compensation claims.

The report outlines a range of measures designed to mitigate these risks, including:

- updated policies and procedures;
- strengthened governance and oversight arrangements;
- revised Authorising Officer structures;
- enhanced social media monitoring controls;
- mandatory training and refresher arrangements;
- quality assurance and compliance review mechanisms;
- quarterly and annual reporting to elected members; and
- incorporation of RIPSAs arrangements within the Council's Strategic Governance Framework and Annual Governance Statement processes.

These risks are managed through ongoing operational oversight by the Senior Responsible Officer, the Information Governance Team, Authorising Officers, and corporate governance arrangements.

5.10 Armed Forces Covenant Duty

Does the report require to take due regard of the Armed Forces Covenant Duty (i.e. does it relate to healthcare, housing, or education services for in-Service or ex-Service personnel, or their families, or widow(er)s)?

Yes No

If Yes, please provide a brief summary of the provision which has been made to ensure there has been appropriate consideration of the particular needs of the Armed Forces community to make sure that they do not face disadvantage compared to other citizens in the provision of public services.

5.11 Children's rights and wellbeing impact

Does the report contain any information regarding any council activity, service delivery, policy, or plan that has an impact on children and young people up to the age of 18, or on a specific group of these?

Yes No

If Yes, please provide a brief summary of the impact and the provision that has been made to ensure there has been appropriate consideration of the relevant Articles from the United Nations Convention on the Rights of the Child (UNCRC).

If Yes, has a Children's Rights and Wellbeing Impact Assessment (CRWIA) been carried out?

Yes No



Policy and Guidelines on Surveillance (RIPSA Policy)

POLICY AND PROCEDURE on DIRECTED
SURVEILLANCE, USE OF COVERT HUMAN
INTELLIGENCE SOURCES AND SOCIAL MEDIA
USAGE



Document control			
Title	Policy and Guidelines on Surveillance		
Owner	Colette Cameron	Contact	CameronCol@northlan.gov.uk
Governance Group	Information Governance, Legal and Democratic Services		
Author	Colette Cameron	Contact	CameronCol@northlan.gov.uk

Revision History			
Number	Originator	Date Review Commenced	Revision description/record of change

Document Approvals			
Number	Governance Group	Date approval granted	Date approval to be requested (if document still draft)
	Policy and Strategy Committee		22 April 2026
	Policy and Strategy Committee	8 June 2023 Document.ashx	
	Policy and Strategy Committee	1 October 2020 Document.ashx	
	Policy and Resources Committee	8 March 2012 Document.ashx	
	Policy and Resources Committee	19 September 2006 Document.ashx	

Consultation Record (for most recent update)	
Status of document consulted upon	
Stakeholders consulted/date	

Strategic Alignment

Next review date	
Review Date	

Policy and Guidelines on Surveillance

(1) Introduction

In some circumstances, it may be necessary for Council employees, in the course of their duties, to make observations of a person(s) in a covert manner, i.e. without that person's knowledge, or to instruct third parties to do so on the Council's behalf. Actions of this sort are potentially intrusive. The Human Rights Act 1998 which came into force in October 2002, gave domestic effect to the European Convention on Human Rights ("the Convention"). Section 6 of the 1998 Act states that all public authorities must act in a manner compatible with the rights contained in the Convention. Article 8 of the Convention affords everyone the right to respect for private and family life including home and correspondence. Surveillance activities by public authorities may therefore result in a legal challenge in terms of Article 8.

Article 8 of the Convention is not however an absolute right. Interference with this right of privacy may be justified if this is:

- in accordance with the law;
- necessary to pursue a legitimate aim, for example, the public interest; and
- the interference is proportionate to the legitimate aim, i.e. the interference with the right is not greater than is necessary to achieve the aim.

The Regulation of Investigatory Powers (Scotland) Act 2000 ("RIPSA") provides, a legal framework for covert surveillance by public authorities and an independent inspection regime to monitor these activities. The primary purpose of RIPSA is to ensure compliance with Article 8 in relation to covert surveillance. Therefore, if RIPSA is properly complied with, any interference with the right to privacy, will be in accordance with the law. In order to put forward a robust defence to any claim by an individual of wrongful interference with their right to privacy under Article 8 of the European Convention on Human Rights, any surveillance type activities undertaken by a local authority must be both necessary and proportionate.

(2) Objectives

The objective of this policy is to ensure that all covert surveillance by Council employees is carried out appropriately and on a lawful basis. This policy should be read in conjunction with the Scottish Government's Covert Surveillance and Property Interference Code of Practice 2017, which is covered in

Part One of this Policy, and Covert Human Intelligence Sources Code of Practice 2017 which is covered in Part Two.

If the procedures outlined in this policy are not followed, any evidence acquired as a result of surveillance activities may be susceptible to legal criticism and challenge. It may additionally not be admissible in Court, and the Procurator Fiscal is unlikely to take proceedings on the basis of such evidence. The Council may also be exposed to legal actions by individuals who claim that their human rights to privacy and respect for family life will have been abused.

(3) Scope of the Policy

The policy only applies where surveillance is covert i.e. where the individual or individuals are not aware at the time of surveillance that surveillance is being carried out. It does not apply to observations or surveillance which are not carried out covertly, e.g., use of overt CCTV cameras or unplanned observations made as an immediate response to events. The Information Commissioner has issued separate [guidance of the use of CCTV surveillance](#).

(4) Review of the Policy

This policy shall be reviewed and set annually by elected members.

PART 1 – Directed Surveillance

1.1 DEFINITION OF DIRECTED SURVEILLANCE

The Regulation of Investigatory Powers (Scotland) Act 2000 defines directed surveillance as surveillance which is covert but 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.

The terms of this Policy apply in all cases where “directed surveillance” is being planned or carried out by Council Officers.

1.2 EXPLANATION OF INTRUSIVE SURVEILLANCE

The Regulation of Investigatory Powers (Scotland) Act 2000 does not permit the authorisation by Council officers of intrusive surveillance. As a matter of policy, local authorities **must not** engage in intrusive surveillance. It is therefore of utmost importance that employees are completely clear as to the definition of intrusive surveillance.

Surveillance is intrusive where it is covert and -

- (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 as carried out by means of a surveillance device.

Some additional points should be made about intrusive surveillance. Residential premises are not thought to include common areas such as common stairs and closes. Surveillance is not intrusive if directed into a home or private vehicle from outside unless the information is consistently of the same quality as would be produced by a device actually sited in the home or vehicle in question. Advice from the Investigatory Powers Commissioner's Office suggests that the sort of surveillance undertaken by the Council is unlikely to reach this level of sophistication, however, this will clearly be subject to review in the future. Thus, activities such as filming goods being sold from the back of a car or monitoring the level of noise (but not the actual words) generated by an anti-social person are unlikely to be classified as intrusive, and so, those activities can be safely carried out subject to appropriate authorisation. Furthermore, devices carried into a home or a private vehicle by a covert human intelligence source (see Part 2 of this Policy) do not constitute intrusive surveillance as long as the CHIS has been invited in. However, the device must not be left behind when CHIS leaves the premises or vehicle.

1.3 PRINCIPLES OF DIRECTED SURVEILLANCE

In planning and carrying out directed surveillance, Council employees must comply with the following principles:

- **lawful purposes** - directed surveillance shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in RIPSAs) i.e., it must be: -
 - (a) for the purpose of preventing or detecting crime or the prevention of disorder;
 - (b) in the interest of public safety;
 - (c) for the purpose of protecting public health; or

Employees carrying out surveillance should not cause damage to any property or harass any person.

- **necessity** - directed surveillance should only be undertaken where there is no reasonable and effective alternative way of achieving the required objective.
- **effectiveness** - planned directed surveillance should be undertaken only by, or under the supervision of, suitably trained or experienced employees.
- **proportionality** - the use and extent of directed surveillance should not be excessive, i.e. it shall be in proportion to the significance of the matter being investigated.
- **intrusive surveillance** - no surveillance should be undertaken which comes within the definition of "intrusive surveillance".

- **collateral intrusion** - specific consideration should be given at both the application and authorisation stages, to the extent of any risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation. Measures should be taken, wherever practicable, to avoid or minimise unnecessary intrusion into the lives of those not directly connected with the investigation or operation.
- **authorisation** - all directed surveillance must be authorised in accordance with the procedures described below.
- **confidentiality** - all directed surveillance should be undertaken in such a way as to minimise, wherever possible, the acquisition of confidential material.

1.4 MAKING AN APPLICATION FOR DIRECTED SURVEILLANCE

Any officer whose duties involve directed surveillance who wishes to carry out directed surveillance must make an application seeking authorisation to do so. Services may require, in the course of their operation or of directed surveillance duties from time to time, to make and consider applications for authorisations. Any overt observations do not require authorisation under RIPSAs.

(a) **When is Directed Surveillance Appropriate?**

By its very nature, directed surveillance intrudes on people's privacy. It should therefore be regarded as a final option, only to be considered when all other methods have either been tried and failed, or where the nature of the activity to which the surveillance relates is such that it can be reasonably concluded that no alternative action will yield the information sought. For example, if a vending machine is regularly being broken into, consideration should be given to installing overt CCTV cameras with appropriate signage before installing hidden cameras.

Another example may be where a Trading Standards Officer covertly observes and then visits a shop as part of their enforcement function to verify the supply or level of goods or services that may be liable to restriction. Such an observation could involve the use of equipment, such as binoculars or the use of cameras where this does not involve a systematic surveillance of an individual. Each case must be taken on its own merits.

Any use of covert surveillance must be proportionate to the objective being pursued – for the purposes of a specific investigation or a specific operation.

(b) **Directed Surveillance**

Authorisation levels are prescribed by the Regulation of Investigatory Powers (Prescription of Officers, etc. and Specification of Public Authorities) (Scotland) Order, SS1 2010/350. In relation to local authorities, the Regulations refer to Assistant Head of Service and Investigation Manager, titles which are little used within local authorities.

The Council's equivalent to an "assistant Head of Service" is a third tier Council officer, for example, a Legal Manager within Legal and Democratic Solutions.

It is felt that the most likely local authority equivalent to an "Investigation Manager" would be the Council's Trading Standards Manager or an equivalent post within another Council Service.

If in any doubt about the level of seniority of a proposed authorising officer in any particular case, specific advice should be sought from the Chief Officer of Legal and Democratic.

Applications must be made in writing using the approved forms, copies of which are available on Connect. In urgent cases, however, an oral application may be approved by an Authorising Officer. Where an urgent application is made this should be supplemented by a normal written application as soon as practicable and in any event within 72 hours failing which the oral authorisation will expire. A written application for directed surveillance should describe any conduct to be authorised as well as the purpose of the investigation or operation. It is recommended in the Code of Practice that the application include the following –

- The reasons why the authorisation is necessary in the intelligence case and on the grounds listed within Section 6 (3) of RIPSAs;
- The nature of the surveillance;
- The identities, if known, of the subjects of the surveillance;
- A summary of the intelligence case and the appropriate unique intelligence references where applicable;
- An explanation of the information hoping to be obtained from the surveillance;
- The details of any potential collateral intrusion and why the intrusion would be justified;
- The details of any confidential information that is likely to be obtained as a consequence of the surveillance;
- If the purpose, or one of the purposes, of the authorisation is to obtain information which is subject to legal privilege, an assessment of why there are exceptional circumstances that make this necessary;
- The reasons why the surveillance is considered proportionate to what it seeks to achieve;
- the level of authorisation required (or recommended where that is different) for the surveillance.

Before the application can be granted, the authorising officer must be satisfied that the surveillance is necessary, that the action is proportionate with what it seeks to achieve and that the aim could not have reasonably been achieved by any other means. The Authorising Officer should note the time and date of the grant/refusal of the application on the relevant form. A Schedule of the Council's designated Authorising Officers is included at Appendix 1.

Authorising officers should not normally be responsible for authorising operations in which they are directly involved. Where an authorising officer authorises such an investigation or operation this should be recorded in the Central Record of Surveillance Activities.

1.5 GRANTING AND RECORDING AUTHORISATIONS AND REFUSALS

The Authorising Officer's job is to be satisfied that the directed surveillance is necessary and that the applicant has correctly identified the lawful purpose for the proposed surveillance, has planned the operation properly so as to minimise collateral intrusion (invasion of privacy of individuals who are not the subject(s) of the surveillance being carried out) and the collection of confidential information, is not proposing to stray beyond permissible bounds of directives and has correctly applied the proportionality test. The authorisation should be granted only if the Authorising Officer is satisfied that these issues have been properly considered, surveillance is justified, and the application conforms with

the Statutory Code of Practice. Any restrictions imposed on the authorisation should be noted as authorising officer comments.

1.6 RECEIPT AND LOGGING OF APPLICATIONS

All Services carrying out surveillance activities must forward all relevant documentation to the Chief Officer of Legal and Democratic so that the Central Register of Surveillance Activities carried out by the Council can be maintained. This confidential register will be open to inspection by the Investigatory Powers Commissioner's Office and provides evidence of the Council's compliance with the law and the Scottish Government's Codes of Practice. The arrangements for updating the Central Register are set out in Appendix 2 of this Policy.

1.7 DURATION, RENEWAL AND CANCELLATION OF AUTHORISATIONS

An authorisation for directed surveillance is valid for a period of three months or, in the case of urgent oral applications, 72 hours. However, if the reasons justifying carrying out the surveillance cease to apply prior to the expiry of a three-month period or a 72-hour period, whichever is applicable, then the authorisation should be cancelled and the cancellation form forwarded to the Chief Officer (Legal and Democratic) for filing in the Central Register.

On approving the authorisation, a planned review date shall be fixed to monitor the effectiveness of the surveillance and its continuing necessity and proportionality.

If surveillance is to be continued for longer than the original period authorised, it is necessary to have a renewal authorised. The tests applicable to renewals are identical to those for initial applications (Forms for [cancellation](#) and [renewal](#) of surveillance are available).

1.8 NECESSITY AND PROPORTIONALITY

RIPSA, read alongside the RIPSA Codes of Practice, provides the statutory framework within which public authorities may lawfully authorise covert surveillance. Compliance with RIPSA does not only require the completion of an authorisation form; it requires a substantive and reasoned assessment that the proposed activity constitutes a necessary and proportionate interference with an individual's rights under Article 8 of the European Convention of Human Rights (ECHR). Article 8 protects an individual's right to respect for private and family life, home and correspondence. Any interference with this right must therefore be in accordance with the law, in pursuit of a legitimate aim and necessary and proportionate. Obtaining an authorisation under RIPSA will only ensure a justifiable interference with Article 8 rights where the Authorising Officer is satisfied that these tests are met in the particular circumstances of the case. Therefore, the use and extent of covert surveillance should not be excessive. RIPSA

Necessity

first requires that the person granting an authorisation is satisfied that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in Section 6 (3) of RIPSA for directed surveillance. Section 6 (3) provides that an authorisation is necessary on the following grounds: -

- (a) for the purpose of preventing or detecting crime or preventing disorder;
- (b) in the interest of public safety;
- (c) for the purpose of protecting public health; or

The Authorising Officer must be satisfied that surveillance is necessary in the circumstances of the specific case, and that the objective cannot reasonably be achieved without covert surveillance. The Code of Practice makes clear that covert surveillance must not be undertaken as a matter of routine and should only be used where other less intrusive methods have failed, are unlikely to succeed or are not practicable.

Proportionality

Where necessity is established, the Authorising Officer must then consider whether the proposed surveillance is proportionate to what is sought to be achieved. Proportionality requires a careful balancing exercise between: -

- the intrusiveness of the surveillance (on the subject and on any collateral individuals); and
- the operational need and seriousness of the matter under investigation.

Surveillance will not be proportionate if its scale, duration or intensity is excessive in relation to the suspected activity, or where the same information could reasonably be obtained by less intrusive means.

When assessing proportionality, Authorising Officers must consider the nature and seriousness of the alleged conduct in the context of the local authority's regulatory and enforcement responsibilities. Low-level or minor breaches, particularly where informal or overt enforcement options remain available, are unlikely to justify covert surveillance. In some cases, sentencing powers associated with criminal offences may assist in assessing seriousness.

However, Authorising Officers should recognise that some regulatory offences enforced by local authorities may carry significant risks to public safety or public health. For example, matters relating to unsafe housing conditions, illegal trading practices, the sale of contaminated food, environmental hazards, or dangerous goods may have serious or life-threatening consequences. In such cases, covert surveillance may be proportionate despite the regulatory nature of the offence.

When seeking an authorisation for directed surveillance, the following must be clearly addressed within the application: -

- **Balancing the activity against the alleged offence**
Demonstrating that the proposed surveillance is commensurate with the gravity and extent of the suspected crime, offence or breach of regulatory requirements.
- **Minimising intrusion**
Explaining how and why the methods proposed represent the least intrusive means of obtaining the required information, and how collateral intrusion will be minimised.

- **Appropriate use of RIPSAs powers**

Confirming that the activity represents a reasonable and proportionate use of RIPSAs powers within the local authority's statutory remit.

- **Consideration of alternatives**

Evidencing, where reasonably practicable, what alternative options (including overt regulatory or enforcement powers) were considered and why they were not adopted.

Necessity and proportionality are not one-off assessments. Authorising Officers retain a continuing responsibility to ensure that authorised surveillance remains justified throughout its duration. Regular reviews must consider whether: -

- the surveillance continues to be necessary;
- the level of intrusion remains proportionate; and
- the objectives have been met or can now be achieved by other means.

The Authorising Officer should focus on confirming that necessity and proportionality as well as the extent and management of collateral intrusion, are adequately addressed, with a clear authorisation statement.

Surveillance must be cancelled as soon as it is no longer necessary or proportionate.

The Code of Practice emphasises that covert surveillance must never be arbitrary or unfair. Activities should be tightly focused, carefully managed, and limited to what is strictly required to achieve the stated objective.

This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms. The activity will not be proportionate if it is excessive in the circumstances of the case or if the information which is sought could reasonably be obtained by other less intrusive means. All such activities should be carefully managed to meet the objective in question.

1.9 CONFIDENTIAL MATERIAL AND COLLATERAL INTRUSION

Confidential material covers a number of areas: professional legal advice, health information, spiritual counselling and material held under an obligation of confidentiality. So far as possible, surveillance operations should be designed so as to minimise or eliminate the possibility of confidential information being acquired. Confidential material should be destroyed once it is no longer necessary for the specific purpose of the surveillance. In particular, the proportionality considerations should always be applied. If confidential information is in fact acquired, special care should be taken to avoid unnecessary disclosure.

Before authorising surveillance, the Authorising Officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation ("collateral intrusion"). Operations should be planned so as to minimise or eliminate as far as possible the risk of collateral intrusion, and the extent to which it remains is a factor to consider when determining the proportionality of the operation. Where recovery of such material is anticipated

and unavoidable, it is a requirement that authorisation for surveillance must be sought from the Chief Executive or, in his absence, the Chief Officer of Legal and Democratic.

1.10 SURVEILLANCE BY OTHER PUBLIC AUTHORITIES AND COMBINED AUTHORISATIONS

Council officers are occasionally asked to assist in surveillance operations being conducted by other public authorities such as the police, the Department for Work and Pensions, other local authorities, HMRC etc. In cases where the Council is acting on behalf of another agency, it is normally for the tasking agency to obtain or provide authorisation. In such cases it is for the tasking agency (who are seeking assistance from the Council) to ensure that it has appropriate authorisations in place. Written confirmation should be obtained from the tasking agency and exhibited to the Council's appropriate authorising officer confirming that such authorisations have been duly granted.

1.11 USE OF SOUND RECORDING EQUIPMENT

Where it is considered necessary for an investigating officer to record levels of noise as part of directed surveillance activity this may involve the use of noise recording equipment. When using such technical equipment investigating officers must ensure that the equipment is activated in such a way as to record only the level of the noise in question and not the actual content of any conversation between the subject of directed surveillance and any other party.

1.13 SAFEGUARDS

Information obtained under a directed surveillance authorisation must be handled in accordance with the safeguards set out below and elsewhere in this policy and the Code of Practice.

Dissemination, copying and retention of information must only be carried out where necessary for the authorised purposes. The authorised purposes are that the material: -

- is, or is likely to become, necessary for any of the statutory purposes set out in RIPSAs;
- is necessary for facilitating the carrying out of the functions of public authorities under RIPSAs;
- is necessary for the facilitating the carrying out of any functions of the Investigatory Powers Commissioner (IPC) or the Investigatory Powers Tribunal (IPT);
- in necessary for legal proceedings;
- is necessary for the performance of any person by or under any enactment.

The information should only be copied and/or disclosed to the minimum people necessary (including internally within the Council) and to the minimum extent necessary for the authorised purposes i.e. if a summary or extract of the information can be disclosed instead of the entirety of the information, then this should be all that is disclosed. Similarly, information should only be copied to the minimum extent necessary for the authorised purposes.

When material is to be used, or may need to be used, as evidence in criminal proceedings, consideration should be given to the evidential integrity, the rules of evidence and disclosure, and it should be borne in mind that the Council will need to show how the material was obtained.

Authorisations should be reviewed regularly to assess necessity and proportionality – this is particularly important where the directed surveillance is likely to involve a high level of intrusion into a person's private life, a high degree of collateral intrusion or where sensitive information is likely to be obtained.

The Council's Data Protection policy must be complied with in respect of any personal data or special category data obtained as part of the investigation.

The information should be stored securely to minimise the risk of loss and theft and should only be accessible to those authorised to access it.

Information should be destroyed securely and in accordance with the Council's Retention Schedule. The Investigatory Powers Commissioner's Office has statutory powers of inspection, and all records (applications, authorisations, cancellations and refusals) must be available for inspection. No records should be destroyed until an inspector has had the opportunity to see them.

The Chief Officer (Legal and Democratic) shall ensure that the Central Register is kept secure and shall make proper arrangements for the retention and destruction of documentation in accordance with the requirements of the UK GDPR, the Data Protection Act 2018 and the Code of Practice. It should be noted that refusals as well as approved applications must be retained. The Code of Practice recommends retention of authorisations for five years or longer, if required for ongoing proceedings.

It is advisable to consult the Code of Practice and Legal Solutions if the information likely to be obtained is likely to be subject to legal privilege.

1.14 TRAINING

Each Service is responsible for ensuring that their staff receive adequate training to deal with the authorisation process and any enquiries, guidance to relevant employees and legal advice will be available as required from the Chief Officer (Legal and Democratic).

1.15 COMPLAINTS

In the event of any member of the public being unhappy or dissatisfied with the conduct of any covert surveillance, in addition to the Council's complaints procedure, they have the right to complain to the Investigatory Powers Tribunal.

Details of the complaint's procedure are available for public reference from Legal and Democratic Solutions. Copies of the Complaints Procedure will be made available to the public by post or e-mail if requested.

The Regulation of Investigatory Powers Act 2000 (RIPA) established an independent tribunal. This tribunal has full powers to investigate any complaints and decide any cases within the United Kingdom, including complaints about activities carried out under the provisions of the RIPA. Details of the

relevant complaint procedure can be obtained from the Investigatory Powers Tribunal, PO Box 33220, London, SW1H 9ZQ

Part 2 – Covert Human Intelligence Sources (CHIS)

2.1 DEFINITION OF COVERT HUMAN INTELLIGENCE SOURCE

RIP(S)A 2000 defines a covert human intelligence source as a person who-

- (a) establishes or maintains a personal or other relationship with another person for the covert purpose of facilitating the doing of anything following 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.

The Scottish Government Code of Practice confirms that a source may include individuals referred to as agents, informants and officers working under cover. A purpose is covert in relation to the establishment and or maintenance of a personal or other relationship only if the relationship is conducted in a manner that is calculated to ensure that one of the parties to the relationship is unaware of the purpose. By virtue of Section 1(8)(c) of RIP(S)A, a relationship is used covertly, and information obtained as above is disclosed covertly, if and only if it is 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. The use of a source involves inducing, asking or assisting a person to engage in the conduct of a source or to obtain information by means of the conduct of such a source. Conduct of a source will include any activities involving the use of or actions of a covert human intelligence source (CHIS) specified in any authorisation. It includes conduct by the CHIS or in relation to the CHIS and where it is carried out for the purposes of or in connection with the specific investigation in question. Any surveillance which is carried out by means of a surveillance device in relation to anything taking place on any residential premises or in private vehicle; but is carried out without that device being present on the premises or in the vehicle (i.e. from a different location) is not intrusive unless that device is such that it consistently provides information of the same quality and detail as might be expected to be obtained from a device actually present on the premises or in the vehicle (Section 1(5) of the Act).

2.2 THE PRINCIPLES OF USE OF COVERT HUMAN INTELLIGENCE SOURCES

The use and management of a Covert Human Intelligence Source (CHIS) engages an individual's right to respect for private and family life under Article 8 of the European Convention on Human Rights. Any interference with this right must be lawful, necessary and proportionate. Compliance with the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) and the associated CHIS Code of Practice is therefore fundamental when considering the authorisation, conduct, management and review of CHIS activity.

When using or seeking to use covert human intelligence sources Council employees must comply with the following principles: -

(a) Lawful purposes - use of covert human intelligence sources shall only be carried out where necessary to achieve one or more of the permitted purposes (as defined in RIP(S)A) which are: -

- preventing or detecting crime or preventing disorder;
- in the interest of public safety; or
- for the purpose of protecting public health.

Employees carrying out surveillance shall not cause damage to any property or harass any person while conducting the surveillance. No authorisation for the conduct or use of a covert human intelligence source should be granted unless one of the three grounds specified above are established.

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

(c) Proportionality – the use and extent of covert surveillance shall not be excessive i.e. it shall be in proportion to the significance of the matter being investigated.

(d) Intrusive surveillance – no activity shall be undertaken that comes within the definition of “intrusive surveillance”, i.e. if it involves surveillance of anything taking place within residential premises or in a private vehicle.

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

2.3 AUTHORISATION OF COVERT HUMAN INTELLIGENCE SOURCE

The process for granting authorisations for the use or conduct of CHIS is the same as for directed surveillance although there is a specific form of application. Copies of the relevant application, renewal and calculation of CHIS forms are attached at Appendix 2. In addition, however, authorisations for use of a CHIS can only be granted if sufficient arrangements have been in place for handling the source's case. The arrangements therefore considered necessary are that: -

- (a) there will at all times be an appropriate officer within the Council who will have day to day responsibility for dealing with the source on behalf of the Council, and for the security and welfare of the source (“the handler”).
- (b) there will at all times be another appropriate person within the Council who will have general oversight of the use made of that source (“the controller”).
- (c) there will at all times be an appropriate person within the Council who will have responsibility for maintaining a record of the use made of the source.
- (d) the records relating to the source are maintained by an appropriate person within the Council and such records will always contain particulars of all such matters as may be specified by regulations made from time to time by the Scottish Ministers (clearly, this requirement should be reviewed on a corporate basis at regular intervals).
- (e) records maintained by the Council which disclose the identity of the source will not be available to persons except to the extent that there is a need for access to them to be made available to those persons.

It is best practice that the officers identified as the handler and controller are named in authorisations.

2.4 GRANTING AND RECORDING AUTHORISATIONS AND REFUSALS

The Authorising Officer’s job is to be satisfied that the use or conduct of a covert human intelligence source is necessary and that the applicant has correctly identified the lawful purpose for the proposed use, has planned the operation properly so as to minimise collateral intrusion and the collection of confidential information. Where the collection of such information is considered likely the application should be authorised by the Council’s Chief Executive. The proportionality test must clearly be satisfied. The authorisation should be granted only if the Authorising Officer is satisfied that these issues have been properly considered and that the application conforms with the Statutory Code of Practice and that use of a CHIS is justified. Any restrictions imposed on the authorisation should be noted as authorising officer comments.

A risk assessment **must** be carried out before a CHIS is authorised to identify the risks to the CHIS and the likely consequences if the identity of the CHIS becomes known. This should consider the risks specific to each authorisation and be updated to reflect developments during the course of the deployment (and after if contact is maintained). The ongoing security and welfare of the CHIS after the deployment should be considered as part of the risk assessment and throughout the deployment. If there is likely to be a requirement to disclose information which may require the identity of the CHIS to be disclosed, this should also be considered.

2.5 RECEIPT AND LOGGING OF APPLICATIONS

All Services carrying out CHIS activities must forward all relevant documentation to the Chief Officer (Legal and Democratic) so that the Central Register of CHIS activities

carried out by the Council can be maintained. This confidential register will be open to inspection by the Investigatory Powers Commissioner's Office and provides evidence of the Council's compliance with the law and the Scottish Government's Codes of Practice. The arrangements for updating the Central Register are set out in Appendix 2 of this Policy.

2.6 DURATION, RENEWAL AND CANCELLATION OF AUTHORISATIONS

A written authorisation for conduct and use of a CHIS is valid for 12 months or 72 hours in the course of an urgent oral authorisation. Applications for the renewal of the conduct or use of a CHIS should not be granted unless the authorising officer is satisfied that a review has been carried out of the use made of the source and the period since the grant, the tasks given to the source during the period and the information obtained from the conduct or use of the source and unless he or she has considered the results of such a review. The authorisation should be cancelled if the person who granted or last renewed an authorisation is satisfied that the authorised conduct is no longer required or no longer satisfies the purpose for which it was granted.

If the reasons justifying carrying out the use of a CHIS cease to apply, then the authorisation should be cancelled and the cancellation form forwarded to the Chief Officer of Legal and Democratic for filing on the Central Register. On approving the authorisation, a planned review date should be fixed to monitor the effectiveness of the use or conduct of the CHIS and its continuing necessity and proportionality.

If surveillance is to be continued for longer than the original period authorised, it is necessary to have a renewal authorised. The test applicable to renewals are identical to those for initial applications.

2.7 WHEN IS THE USE OF A CHIS APPROPRIATE?

By its very nature the use of a CHIS intrudes on the privacy of individuals, perhaps even more so than in the case of directed surveillance. It must be regarded as the final option to recover information only to be considered when all other methods have either been tried and failed or where the nature of the activity to which the surveillance relates is such that it can be reasonably concluded that no alternative action will yield the information sought. For example, if a vending machine is regularly broken into consideration should be given to installing overt CCTV cameras (with appropriate signage) before installing hidden cameras. Any use of a CHIS must be proportionate to the objective being pursued.

2.8 ONLINE COVERT ACTIVITY

Where Council officers are interacting with individuals online, either via publicly open websites or more private communications, where those individuals are not reasonably likely to know the true identity of the Council officer, consideration should be given to whether a CHIS authorisation is required.

If an investigation or operation requires a covert relationship with an individual or a group of people online to be established in order to gain access to information, a CHIS authorisation will likely be required e.g. using the internet to engage with an individual in order to facilitate a meeting in person. If no relationship is being established, then a CHIS authorisation may not be required immediately e.g. if a false identity needs to be set up to access a website (consideration should be given to whether a directed surveillance authorisation is required) or “liking” or “following” someone. It would only be once that interaction increased so as to start obtaining or accessing information that a CHIS authorisation would be required.

If there is any dubiety over whether an authorisation is required, advice should be sought from Legal and Democratic prior to the investigation commencing.

Any risk assessment carried out in accordance with section 6.13 of the Covert Human Intelligence Source Code of Practice should include consideration of the risks arising from the online activity including the length of time spent online and the material to which the CHIS may be exposed. If an online persona is going to be used by multiple officers, separate risk assessments for each officer should be carried out (as well as separate authorisations sought).

2.9 NECESSITY AND PROPORTIONALITY

Necessity

RIP(S)A requires that an authorisation for the use or conduct of a CHIS is necessary in the circumstances of the particular case. Necessity must not be assumed as a matter of routine and cannot be justified by general operational convenience. The authorising officer must be satisfied that the use of a CHIS is required for at least one of the statutory grounds set out in Section 6.3 of RIP(S)A, namely: -

- For the purpose of preventing or detecting crime or preventing disorder;
- In the interests of public safety;
- For the purpose of protecting public health.

The assessment of necessity must demonstrate a clear operational requirement for covert activity. Consideration must be given to whether the intelligence or outcome sought is essential to achieving the legitimate aim and whether that aim is of sufficient seriousness to justify the intrusion. The use of a CHIS should only be considered where overt methods or less intrusive investigative techniques have either been tried and failed, would be ineffective, or would be impractical or likely to compromise the investigation. Necessity must also be kept under continuous review. If at any stage the original justification no longer applies, the authorisation must be cancelled.

Obtaining an authorisation under RIP(S)A will only ensure that there is a justifiable interference with an individual's Article 8 rights if it is necessary and proportionate for these activities to take place. RIP(S)A first requires that the person granting an authorisation is satisfied that the authorisation is necessary in the circumstances of the particular case for one or more of the statutory grounds in Section 6.3 of RIP(S)A in the use of a CHIS. Section 6.3 provides that an authorisation is necessary.

Then, if the activities are necessary, the person granting the authorisation must be satisfied that they are proportionate to what is sought to be achieved by carrying them out. This involves balancing the intrusiveness of the activity on the target and others who might be affected by it against the need for the activity in operational terms.

Proportionality

Where necessity is established, the authorising officer must then be satisfied that the proposed CHIS activity is proportionate to what is sought to be achieved. Proportionality requires a careful balancing exercise between: -

- The level and extent of intrusion into the private life of the subject of the CHIS activity; and
- The operational benefit and importance of the information or outcome sought.

An activity will not be proportionate if it is excessive in relation to the seriousness of the matter under investigation, or if the same result could reasonably be achieved through less intrusive means. Authorising officers must consider not only the impact on the intended subject but also the potential for collateral intrusion, including the effect on family members, associates, or other third parties who may be incidentally affected by the CHIS activity.

Proportionality also requires that CHIS activity is: -

- Targeted and precise, avoiding general or speculative intrusion;
- Limited in duration, scope and scale to what is strictly required;
- Actively managed and supervised to ensure it remains within authorised parameters.

In line with the CHIS Code of Practice, all CHIS activity must be conducted in a manner that is fair, non-arbitrary and properly controlled. The authorisation process must not be used to legitimise disproportionate or unjustified interference with private life. Appropriate arrangements must be in place for: -

- The management and handling of the CHIS;
- Ongoing risk assessment, including risks to the CHIS and others;
- Regular review and renewal of authorisations, ensuring that necessity and proportionality continue to be met.

The lawful use of a CHIS under RIP(S)A depends not merely on the existence of an authorisation, but on the quality and robustness of the decision-making behind it. Authorising officers must be satisfied that: -

- The activity pursues a legitimate statutory purpose;
- The use of a CHIS is strictly necessary in the particular circumstances;
- The intrusion is proportionate, controlled and no more than is required to achieve the intended outcome; and
- The activity is fair, justified and subject to effective oversight.

Only where all these requirements are demonstrably met will an interference with Article 8 rights be capable of being justified under RIP(S)A.

2.10 CONFIDENTIAL MATERIAL AND COLLATERAL INTRUSION

Confidential material covers a number of areas: professional legal advice, health information, spiritual counselling and material held under an obligation of confidentiality. So far as possible, use or conduct of a CHIS operation should be designed so as to minimise or eliminate the possibility of confidential information being acquired. If confidential information is in fact acquired, special care should be taken to avoid unnecessary disclosure.

Before authorising use or conduct of a CHIS, the authorising officer should also take into account the risk of intrusion into the privacy of persons other than those who are directly the subjects of the investigation or operation (collateral intrusion). Operations should be planned so as to minimise or eliminate as far as possible the risk of collateral intrusion, and the extent to which it remains is a factor to consider when determining the proportionality of the operation. Where recovery of such material is anticipated and unavoidable, it is a requirement that authorisation for use or conduct of a CHIS must be sought from the Chief Executive or, in his absence, the Chief Officer (Legal and Democratic).

2.11 SAFEGUARDS

Material obtained by a CHIS must be handled in accordance with the safeguards set out below and elsewhere in this policy and the Code of Practice.

Dissemination, copying and retention of material must only be carried out where necessary for the authorised purposes. The authorised purposes are that the material: -

- is, or is likely to become, necessary for any of the statutory purposes set out in RIPSAs;
- is necessary for facilitating the carrying out of the functions of public authorities under RIPSAs;
- is necessary for the facilitating the carrying out of any functions of the IPC or IPT;
- is necessary for legal proceedings;
- is necessary for the performance of any person by or under any enactment.

The material should only be copied and/or disclosed to the minimum people necessary (including internally within the Council) and to the minimum extent necessary for the authorised purposes i.e. if a summary or extract of the material can be disclosed instead of the entirety of the information, then this should be all that is disclosed. Similarly, information should only be copied to the minimum extent necessary for the authorised purposes.

If material is disclosed to third parties, consideration should be given to what appropriate safeguards should be applied to those third parties.

When material is to be used, or may need to be used, as evidence in criminal proceedings, consideration should be given to evidential integrity, the rules of evidence and disclosure, and it should be borne in mind that the Council will need to show how the material was obtained.

Authorisations should be reviewed regularly to assess necessity and proportionality – this is particularly important where the directed surveillance is likely to involve a high level of intrusion into a person’s private life, a high degree of collateral intrusion or where sensitive information is likely to be obtained.

The Council’s Data Protection policy must be complied with in respect of any personal data or special category data obtained as part of the investigation.

The material should be stored securely to minimise the risk of loss and theft and should only be accessible to those authorised to access it.

Information should be destroyed securely and in accordance with the Council’s Retention Schedule. The Investigatory Powers Commissioner’s Office has statutory powers of inspection, and all records (applications, authorisations, cancellations and refusals) must be available for inspection. No records should be destroyed until an inspector has had the opportunity to see them.

Documents created under this procedure are highly confidential and shall be treated as such. The Chief Officer of Legal and Democratic shall ensure that the Central Register is kept secure and shall make proper arrangements for the retention and destruction of documentation in accordance with the requirements of the UK GDPR, the Data Protection Act 2018 and the Covert Human Intelligence Source Code of Practice 2022.

It should be noted that refusals as well as approved applications must be retained. The Code of Practice recommends retention of authorisations for five years or longer, if required for ongoing proceedings.

In accordance with guidance issued by the Office of Surveillance Commissioners, documents will be inspected periodically by a senior officer to ensure that a consistent approach is being adopted by different Council Departments. The Investigatory Powers Commissioner’s Office has statutory powers of inspection, and all records (applications, authorisations, cancellations and refusals) must be available for inspection. No records should be destroyed until a Surveillance Commissioner has had the opportunity to see them.

2.12 TRAINING

Each Service is responsible for ensuring that their staff receive adequate training to deal with the authorisation process and any enquiries. Guidance to relevant employees will be issued by the Corporate Working Group and legal advice will be available as required from the Council's Legal and Democratic service.

2.13 COMPLAINTS

In the event of any member of the public being unhappy or dissatisfied with the conduct of any covert surveillance, in addition to the Council’s complaints procedure, they have the right to complain to the Investigatory Powers Tribunal.

Details of the complaint's procedure are available from the Council's Legal and Democratic Solutions. Copies of the Complaints Procedure will be made available to the public by post or e-mail if requested.

Part 3 – Surveillance through Social Media

3.1 INTRODUCTION

This part of the document sets out North Lanarkshire Council's policy in relation to internet surveillance using social media. In some circumstances, it may be necessary for North Lanarkshire Council employees, in the course of their duties, to access social media websites either by creating covert identities or through the officer's Service identity. There are ever increasing and changing types of social media. Such types include (but are not limited to) Facebook, Instagram, TikTok and Snapchat. This guidance refers specifically to Facebook but the principles involved should be applied to dealings with any social media platform that is used in a covert surveillance exercise.

3.2 AIM

The aim of this policy is to provide the framework outlining the Council's process for authorising and managing internet surveillance operations using social media, and to set the parameters for expected good practice. It is important that Council employees effectively carry out surveillance through social media, while remaining in accordance with the law. This policy should be read in conjunction with the relevant legislation, the Codes of Practice and any guidance which the Investigatory Powers Commission may issue from time to time.

3.3 NORTH LANARKSHIRE COUNCIL SOCIAL MEDIA PRESENCE

North Lanarkshire Council has an internet presence as a corporate entity. The corporate entity currently has profiles on Facebook, X (formerly Twitter), Instagram, LinkedIn, TikTok, NextDoor, Flickr and YouTube. Access to these accounts is limited to the Corporate Communications team. Several Council services utilise their own corporate accounts to post information relevant to their activities and events. Individual schools also have their own social media presence.

3.4 TYPES OF INVESTIGATORS' ACCOUNTS AND SURVEILLANCE

There are two different ways in which social media websites may be accessed by Council Officers to carry out investigations:

- Through an identity created specifically as the service's representative.
- Through a cover identity using a false name.

Officers must not use a private social media account whilst carrying out an investigation on behalf of the Council.

Investigators utilise social media in two different ways:

- By simply visiting/viewing third party accounts or groups.
- By entering into a personal relationship with the third party/group member.

Investigators utilising social media should ensure that the Authorising Officer at review, knows the precise extent of online dialogue with a subject. This will be helpful to ensure that there is no drift into establishing a covert relationship, a line that is often imprecise, but one for which the Authorising Officer is accountable.

3.5 PRIVACY SETTINGS OF ACCOUNT UNDER INVESTIGATION

The vast majority of social media websites will have a range of privacy settings that users can apply to protect their accounts from others accessing their information. Facebook is the most commonly used social media website by North Lanarkshire Council Officers to investigate service users or potential service users, and it has several different privacy settings. Depending on what privacy setting a user chooses, different people can access the account and see all or some of its contents.

The different types of privacy settings include:

- 'Public' – all Facebook users can see the account and all its content, including the user's "friends", their timeline and photographs. Non-Facebook users can see photographs and posts published on the account, but not who has 'liked' a post or the marital status or geographic location of the user.

- 'Friends' – only those whom the user has accepted as Facebook 'friends' are able to see the entire content of the user's page.
- 'Custom' - the user can create lists of specific contacts and Facebook users and designate them as the audience for – or block them from view of – any posts.

Of these three options, the relevant options for Investigating Officers are 'public' and 'friends', as option 3 is a sub-category of 'friends'.

3.5 UTILISATION OF SOCIAL MEDIA

Public Privacy Setting

If an Investigating Officer views a service user's Facebook profile, with whom they are not 'Friends', and where the content is not protected by any privacy settings, then information on this profile can be treated as being in the public domain. Any viewing/visiting of this profile on an ad hoc or one-off basis will be overt and no authorisation is required under RIPSAs.

If the Investigating Officer frequently or regularly views/visits the same individual's profile and begins collecting evidence from this, this must be considered as targeted and may constitute directed surveillance. Such actions would be considered on a case by case basis and where appropriate, authorisation under RIPSAs for directed surveillance must be sought.

If an Investigating Officer enters into a 'conversation' with the service user, and if the Officer informs them that they are contacting them in their role as an employee of North Lanarkshire Council, then this contact will be overt, and no authorisation is required under RIPSAs. In any other instance, where the contact is not overt, authorisation for the use and conduct of a CHIS will be necessary.

Friends' privacy setting

To investigate a service user whose Facebook account is protected by privacy settings, the Investigating Officer will be required to send the service user a 'friend request'. As it is obvious from the department name that the person behind the account is a North Lanarkshire Council employee, then the action could not be classified as covert. No RIPSAs authorisation would be needed.

In either of the above privacy settings, although the Investigating Officer has been given access to the account with the consent of the owner, consideration must be given as to whether the account may contain information about others who have not given their consent. If there is a likelihood of obtaining private information about others, the need for a directed surveillance authorisation should be considered, particularly where it is intended to monitor the account going forward.

3.6 SURVEILLANCE USING COVERT IDENTITY

Before an Investigating Officer establishes a relationship with a service user under a covert identity in order to obtain, provide access to, or disclose information, a covert human intelligence source ('CHIS') authorisation will need to be in place.

However, if a covert identity is presented but no steps are taken to form a relationship with the service user, a CHIS authorisation may not be required. For example, where a website or social media account requires a minimum level of interaction (such as sending or receiving a friend request before access is permitted) this may not 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 constitute forming a relationship. More guidance on the use of CHIS powers can be found at Part 2 of this Policy.

3.7 BEST PRACTICES FOR THE USE OF SOCIAL MEDIA IN INVESTIGATIONS

As a matter of best practice, whenever a Council Officer intends to investigate a particular service user through social media, rather than conducting a general sweep of social media websites, an appropriate RIPSAs authorisation should be completed.

3.8 AUTHORISATION FOR ALL TYPES OF SURVEILLANCE

Please refer to North Lanarkshire Council’s Policies and Procedures on Directed Surveillance and Use of Covert Human Intelligence Sources contained in Part 1 and Part 2 of this Policy.

Part 4 – Communications Data

4.1 INTRODUCTION

Part 3 of the Investigatory Powers Act 2016 (‘the Act’) permits certain public bodies to acquire specified types of communications data in limited circumstances, subject to prior authorisation granted in accordance with the Act. Part 3 applies principally to the police and central government departments and agencies, including defence, security and intelligence bodies. The power it grants to local authorities is less extensive, limiting the acquisition of data to cases involving the prevention or detection of serious crime.

The communications data which, in defined circumstances, the Council is permitted to obtain under the Act is known as ‘entity data’ and ‘events data’. Their scope is explained in section 2 below but, in brief, data of this nature can identify who a suspected offender has been in communication with via their telephone or e-mail, as well as where that communication was made or received. The data may therefore be of real investigative benefit.

The legal framework for this policy is the 2016 Act and statutory guidance contained in the Home Office Code of Practice on Communications Data which was last update in 2025.

4.2 Communications Data

In the Act and this policy, the term 'communications data' means 'entity data' and 'events data' and includes the 'who', 'when', 'where', and 'how' of a communication but not the content i.e. what was said or written.

Entity data means any data which is about:

- an entity (a person or thing such as a phone, tablet or computer)
- an association between a telecommunications service and an entity, or
- an association between any part of a telecommunication system and an entity

Entity data will consist of, or will include, data which identifies or describes the entity (whether or not by reference to the entity's location). It is not events data.

Entity data covers information about a person or thing, and about links between a telecommunications system and a person or thing that identifies or describes the person or thing. This means that individual communication devices such as phones, tablets and computers are entities. The links between a person and their phone are therefore entity data but the fact of or information about communications between devices on a network at a specific time and for a specified duration would be events data.

Examples of entity data include:

- subscriber checks
- subscribers' or account holders' account information, including names and addresses for installation, and billing including payment method(s), details of payments;
- information about the connection, disconnection and reconnection of services to which the subscriber or account holder is allocated or has subscribed (or may have subscribed) including conference calling, call messaging, call waiting and call barring telecommunications services;
- information about apparatus or devices used by, or made available to, the subscriber or account holder, including the manufacturer, model, serial numbers and apparatus codes; and
- information about selection of preferential numbers or discount calls.

Events data is more intrusive and means any data which identifies or describes an event (whether or not by reference to its location) on, in or by means of a telecommunication system where the event consists of one or more entities engaging in a specific activity at a specific time. Events data includes the way in which, and by what method, a person or thing communicates with another person or thing. It excludes anything within a communication including text, audio and video that reveals the meaning, other than inferred meaning, of the communication. Events data can also include the time and duration of a communication, the telephone number or email address of the originator and recipient, and the location of the device from which the communication was made.

It covers electronic communications including internet access, internet telephony, instant messaging and the use of applications. Examples of events data include, but are not limited to:

- information tracing the origin or destination of a communication that is, or has been, in transmission (including incoming call records);

- information identifying the location of apparatus when a communication is, has been or may be made or received (such as the location of a mobile phone);
- information identifying the sender or recipient (including copy recipients) of a communication from data comprised in or attached to the communication;
- routing information identifying apparatus through which a communication is or has been transmitted (for example, file transfer logs and e-mail headers – to the extent that content of a communication, such as the subject line of an e-mail, is not disclosed)
- itemised telephone call records (numbers called);
- itemised internet connection records;
- itemised timing and duration of service usage (calls and/or connections); and
- information about amounts of data downloaded and/or uploaded;

4.3 Extent of Data Acquisition Powers

The Council's acquisition of communications data under Part 3 of the Act will be a justifiable interference with an individual's human rights under Article 8 (the right to respect for privacy and family life) of the European Convention on Human Rights only if the conduct being authorised or required to take place is:

- necessary for the purposes of a specific investigation or operation; and
- proportionate

When applying for authorisation to acquire communications data, the Council must believe the acquisition is necessary for the purpose of the prevention or detection of serious crime. 'Serious crime' means:

- an offence for which an adult is capable of being sentenced to one year or more in prison;
- any offence involving violence, resulting in a substantial financial gain or involving conduct by a large group of persons in pursuit of a common goal;
- any offence committed by a body corporate; or
- any offence which involves the sending of a communication or a breach of privacy; or an offence which involves, as an integral part of it, or the sending of a communication or breach of a person's privacy.

The Council must also believe the acquisition to be proportionate to what is sought to be achieved by obtaining the specified communications data – that the conduct is no more than is required in the circumstances.

The Council has **no** power to obtain the content of a communication.

4.4 Roles in Applying for and Granting Authorisation

Acquisition of communications data under the Act involves four roles:

- the applicant

- the single point of contact ('SPoC')
- the Senior Responsible Officer
- the authorising individual

The applicant is a Council officer involved in conducting or assisting an investigation or operation who makes an application in writing or electronically for the acquisition of communications data.

The SPoC is ordinarily an individual trained to facilitate the lawful acquisition of communications data and effective co-operation between the body applying for authorisation (the Council). The Council has decided to utilise the National Anti-Fraud Network (NAFN) Telecommunications services to carry out the SPoC role. This is an online service using the NAFN website and will require all applicants and designated persons to be registered users, along with the Senior Responsible Officer. This reflects the relatively low level of acquisition of communications data and means that the Council will not be required to retain trained officers for this role. The Home Office will deactivate those personal identification numbers held by existing council SPOCs as they will not be required. These SPOC details will remain on the Home Office system so that they can be reactivated at any point should the council cease to rely on the NAFN service.

The Senior Responsible Officer ('SRO') must be a member of the corporate management team. The designated SRO for North Lanarkshire Council is the Chief Officer of Legal and Democratic. The SRO is responsible for:

- the integrity of the process in place within the Council to acquire communications data;
- compliance with Part 3 of the Act and with the Home Office code of practice on communications data;
- oversight of the reporting of errors to the IPC and the identification of both the cause(s) of errors and the implementation of processes to minimise repetition of errors;
- ensuring the overall quality of applications submitted to the Council's SPoC;
- engagement with the IPC's inspectors when they conduct their inspections; and
- where necessary, oversight of the implementation of post-inspection action plans approved by the IPC.

For the Council, the authorising individual is, Chief Officer (Audit and Risk).

4.5 Procedure for Applying for Authorisation to Acquire Communications Data

As with the Procedures for Covert Surveillance, an application for approval to allow communications data to be obtained ("an application") should be completed by the investigator who is involved in the operation in question. It is important to remember that it will be for the investigator to justify any information contained within an application, so extreme care should be taken.

The investigator will have to provide the following information:-

- The name or designation of the applicant;
- The operation and person (if known) to which the requested information relates;
- A description, in as much detail as possible, of the information requested (and whether the information is Service Use or Subscriber information);
- The reason why obtaining the requested data is considered to be necessary for the prevention and detection of crime or prevention of disorder;
- An explanation of why the information constitutes conduct proportionate to what it seeks to achieve;
- Where appropriate, a consideration of collateral intrusion, the extent to which the privacy of others may be affected and why that intrusion (collateral intrusion) is justified; and
- The timescale within which the information is required and why this is justified.

Unlike the Procedures for Covert Surveillance, the application will be considered by the SPOC who can reject it, request further information from the investigator or pass it to the authorising individual for approval.

The SPOC has a regulatory role in connection with the applications for authorisations. They will assess an application to make sure that there is sufficient information contained within it to allow the authorising individual to come to a decision on whether the application should be approved.

If there is insufficient information contained within the application to allow the application to proceed to the authorising individual, the SPOC will at this stage refuse the application and return it, together with an explanatory report to the investigator. The SPOC is not considering the application on its merits as if they were an authorising individual but only the sufficiency of the information being provided by the investigator.

If there is sufficient information, the SPOC will, **before** the application is forwarded to the authorising individual:

- where appropriate assess whether access to communications data is reasonably practical for the Communications Service Provider;

- advise investigators and the authorising individual on the practicalities of assessing different types of communications data from different postal or Communications Service Providers;
- advise applicants and the authorising individuals on whether the data falls within the classes to which the Council can have access;
- provide safeguards for authentication;
- assess any cost and resource implications to both the Council and the Communications Service Provider.

The SPOC will prepare any comments that he/she might have on the application (such as cost etc.) and complete and forward the request for authorisation via the website to the authorising individual.

The SPOC will **not** however be expected to justify any information contained in, or the approval of, any application. This will be a matter for the applicant and the authorising individual respectively.

On receiving an application, the authorising individual must ensure that the requirements of the law are met. Therefore he/she must be satisfied that:-

- the permitted purpose exists; and
- the obtaining of communications data is absolutely necessary; and
- the obtaining of communications data is proportionate; and
- any urgent timescale is justified.

If the authorising individual is not satisfied that all of these conditions are met, they are under a duty to refuse the application. **Remember** that on any challenge it will be the authorising individual who will be required to justify the approval of the application.

The authorising individual is not bound to accept any comments made by the SPOC in relation to the application but should consider them.

4.6 Training for Officers with Designated Roles

The Council must provide an adequate level of initial and refresher training to relevant officers to enable them to perform the role of applicant and SRO. The Council may enter into formal or informal partnership arrangements with other local authorities for the purpose of procuring region-wide training, in the interests of efficiency and effectiveness.

4.7 Retention

The Council must keep records of the appropriate matters set out in the Communications data code of practice, including the number of applications it submits to the SPoC for the acquisition of communications data, how many applications were forwarded for authorisation and, of these, the number granted and declined.

All material obtained through the acquisition of communications data, including all copies, extracts and summaries must be handled and stored securely on Council systems to reduce the risk of loss or theft. Access to the material must be restricted to Council officers undertaking the operation or where necessary as part of the retention process or legal proceedings. All communication data obtained, including copies, extracts and summaries should be scheduled for deletion or destruction and securely destroyed as soon as they are no longer required in accordance with the Council's retention policy.

APPENDIX 1

SCHEDULE OF DESIGNATED AUTHORISING OFFICERS FOR DIRECTED SURVEILLANCE AND COVERT HUMAN INTELLIGENCE SOURCE (“CHIS”) APPLICATIONS

Chief Officer (Legal and Democratic), Chief Officer (Audit and Risk) Chief Officer (Community Operations), Business Manager (Protective Services)

APPENDIX 2

The Chief Officer (Legal and Democratic) is responsible for maintaining the Central Register of Directed Surveillance activities and Central Record of CHIS activities.

Both central registers are stored on the RIPSAs/RIPAs Authorisations Microsoft Teams channel.

Services must ensure that all authorisations, reviews, renewals, cancellations and refusals are uploaded to the designated Microsoft Teams channel as soon as they have been granted. The Information Governance team within Legal Solutions should also be notified of any additions to the central registers by email to DataProtection@northlan.gov.uk.

INTERNET/SOCIAL MEDIA/OPEN SOURCE INVESTIGATIONS

This form should be completed prior to commencing any Internet/Social Media/Open Source (“online”) investigation into an individual where this is required for the purposes of fulfilling one of the Council’s statutory functions e.g. Adult Protection, Planning Enforcement.

The Council’s surveillance of individuals’ private information online, including information which may be made available on e.g. an open social media profile, could be considered intrusive as individuals may still have an expectation of privacy in regards to this information. This may apply even where they have opted to make social media pages on their accounts publicly accessible.

Under Article 8 of the European Convention on Human Rights (ECHR) individuals have a right to respect for their private and family life, their home and correspondence. Section 6 of the Human Rights Act 1998 makes it unlawful for the Council to act in a manner which breaches the ECHR. The purpose of the form is to demonstrate that any online investigation is necessary and proportionate and therefore does not breach an individual’s right to respect for private and family life.

Any use of social media for Council purposes requires to be carried out in accordance with [Acceptable Use of IT Policy.pdf](#) and [Guidance on the use of Social Media for work purposes v2.7 March 2023.pdf](#). **Personal devices and personal social media accounts should not be used to carry out any online investigations for work purposes.**

Use of social media should be actively monitored by managers to ensure any such activity is appropriately authorised.

This form should **not** be used where the online investigation constitutes surveillance which is governed by the Regulation of Investigatory Powers (Scotland) Act 2000 and the Council’s Policy and Procedure on Directed Surveillance, use of CHIS (Covert Human Intelligence Sources) and obtaining Communications Data. If you are unsure about this further advice can be obtained by contacting DataProtection@northlan.gov.uk.

Applicant Name	
Position & Service	
Contact details	

(1) Details of application

Who is the subject of the investigation?	
What checks will be carried out? Specify what online sources will be checked. Specify the nature of the activity (browsing or engaging).	
What is the purpose of the investigation? Specify any statutory function to which this investigation relates.	

Will the checks be one off or repeated?	
Which identity has been used? (Overt or Covert?)	
Outcomes or evidence collected?	

(2) Necessity

Describe why these checks are necessary for the stated purpose?	
What is the impact of not carrying out these checks?	

(3) Proportionality

Can the information be obtained through other less intrusive means?	
If no, explain why not. If yes, explain why these are not being carried out or why these checks remain necessary despite having already carried out those less intrusive means.	
What steps are being taken to minimise the privacy impact on the individual?	
What steps will be taken to reduce or eliminate the checking of information relating to individuals other than the individual who is the subject of the investigation?	

[Authorising] Officer Name	
Signature	
Date	

Use of the Powers	
<p>Please confirm if you have used the covert powers available to you since the last inspection; plan to use them imminently; or can envisage doing so, e.g. following the formation of a new investigative team or strategy:</p>	<p>Since the last inspection in 2023, covert powers have been utilised by the Protective Services team in relation to Directed Surveillance. In total, nineteen Directed Surveillance authorisations have been granted during this period.</p> <p>There has been no use of Covert Human Intelligence Sources (CHIS) powers within the same timeframe.</p> <p>The Council does not currently plan to initiate any further use of covert powers outside of these operational requirements; however, the potential use of such powers may be considered in line with any future investigative strategies or operational requirements, in accordance with statutory authorisation procedures and oversight arrangements.</p>
<p>If you have used the powers, please provide an electronic copy of, a) your Central Record, b) the relevant application, authorisation, any review(s) and cancellation paperwork in your reply:</p>	<p>Electronic copies of the relevant records and documentation are provided with this response.</p> <p>This includes:</p> <ul style="list-style-type: none"> • Central Record of Applications for Directed Surveillance – Main Register (North Lanarkshire Council). • Copies of the RIP(S)A authorisations and associated documentation for the nineteen Directed Surveillance applications granted since the last inspection. This includes the original applications, authorisations, review documentation and cancellations records where applicable. • Central Record of Applications for Covert Human Intelligence Sources (CHIS). <p>For clarity, while the CHIS central record is provided for completeness, the Council has not made use of CHIS powers since the last inspection in 2023 and therefore no associated applications, authorisations, reviews or cancellations are included.</p>

Response to Last Inspection	
<p>Please provide details and evidence to show how any Areas of Non-Compliance identified at your last inspection have been remedied:</p>	<p>No areas of non-compliance were identified during the Council's previous inspection. Accordingly, no remedial actions were required.</p> <p>The Council has continued to maintain appropriate governance arrangements, policies and oversight mechanisms to ensure ongoing compliance with the requirements of the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) and the associated Codes of Practice.</p>
<p>Please provide details and evidence of any action taken in response to observations or recommendations made at your last inspection:</p>	<p>No formal observations or recommendations were made during the Council's previous inspection. However, the Inspector requested that the Council continue to ensure that key compliance matters receive appropriate internal governance and oversight through the Chief Executive and the designated Senior Responsible Officer. These areas included: policy review and refresh, periodic reporting to Elected Members, ongoing training and awareness raising, internal compliance monitoring by relevant service managers, and appropriate arrangements for the retention, review and destruction (RRD) of material obtained through the use of covert powers in accordance with the safeguards set out in the relevant Codes of Practice.</p> <p>In response, the Council has taken the following steps to maintain and strengthen its compliance arrangements:</p> <ul style="list-style-type: none"> • Policy Review: A revised RIP(S)A Policy has been drafted and is currently undergoing internal review. The updated policy will incorporate further guidance in relation to internet use, social media and open-source investigations, reflecting developments in investigative practice and the relevant Codes of Practice. • Member Oversight: While no annual update has been presented to Elected Members since 2023, it is intended that the revised policy and an accompanying update report will be submitted to the appropriate Committee for consideration in June 2026. • Training: RIP(S)A training for relevant officers and Authorising Officers was delivered by an external training provider on 12 March 2026 and 20 March 2026. These sessions provided refresher training on the statutory framework, authorisation processes and compliance requirements under the legislation. • Ongoing Awareness and Training: The Council intends to continue to provide periodic training and awareness sessions for relevant officers to ensure continued understanding of the legislative framework and the appropriate use of investigatory powers.

	Further information relating to internal compliance monitoring arrangements and the retention, review and destruction of material obtained through covert powers is provided in the relevant sections below.
--	--

Policies and Procedures	
<p>Please provide a copy of your RIP(S)A Policy and confirm, a) the date it was last reviewed, b) the date it was last submitted to your Elected Members for approval:</p>	<p>A copy of the Council's current RIP(S)A Policy is provided with this response.</p> <p>The policy was last reviewed and approved by Elected Members on 8 June 2023.</p> <p>A revised version of the policy is currently being finalised, incorporating updated guidance and reflecting developments in relevant legislation, Codes of Practice and investigative practice, including considerations relating to internet use, social media and open-source investigations.</p> <p>The revised policy, together with an accompanying update report, is scheduled to be presented to the appropriate Committee for consideration and approval in June 2026.</p>
<p>Please provide a copy of any policy relating to RIP(S)A considerations when using the internet or social media as part of investigations / enforcement activity (unless included as part of your main RIP(S)A policy):</p>	<p>Guidance relating to the use of the internet and social media for investigative purposes is currently incorporated within Part 3 of the Council's RIP(S)A Policy. A copy of the policy has been provided as part of this response.</p> <p>A review of the RIP(S)A Policy is currently underway to ensure that it remains aligned with the relevant Codes of Practice and current investigative practice, including the use of internet research, social media and open-source intelligence as part of enforcement and investigative activity.</p> <p>The revised policy is currently being finalised through the Council's internal governance process and will incorporate enhanced guidance in relation to internet, social media and open-source investigations. Once this process is complete, the updated policy will be submitted to the Policy and Strategy Committee for consideration and approval by Elected Members.</p>

Training	
<p>Please confirm, a) the name and job title of your RIP(S)A Senior Responsible Officer and Authorising Officer(s), b) the date each of these officers last completed RIP(S)A training:</p>	<p>The Council's Senior Responsible Officer (SRO) for RIP(S)A is Rachel Blair, Chief Officer (Legal and Democratic).</p> <p>The Council's RIP(S)A Policy identifies the following officers as Authorising Officers: Rachel Blair (Chief Officer, Legal and Democratic), Francis Scott (Chief Officer, Audit and Risk), Lyall Rennie (Chief Officer, Community Operations), Andrea Breen, Karen Workman and Margaret Flavell (Senior Managers, Adult Social Work Services), Paul Bannister (Business Manager, Regulatory Services), Lorna Bowden (Planning and Place Manager, Enterprise and Communities), and Siobhan Hughes (Senior Education and Families Manager, Social Work) (Justice).</p> <p>The Council's Business Management Team has considered and agreed the proposed Authorising Officer arrangements comprising the Chief Officer (Legal & Democratic), Chief Officer (Audit & Risk), Chief Officer (Community Operations), and the Business Manager (Regulatory Services), and the revised RIP(S)A Policy will reflect this structure.</p> <p>RIP(S)A training for the Senior Responsible Officer and Authorising Officers was most recently delivered by an external provider on 12 March 2026 and 20 March 2026. These sessions provided refresher training on the legislative framework, authorisation processes, and compliance requirements under the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A) and the associated Codes of Practice.</p>
<p>Please provide details of any RIP(S)A training or awareness raising provided to wider council staff since your last inspection:</p>	<p>Since the last inspection, the Council has arranged refresher RIP(S)A training for relevant staff. This training was delivered by an external provider on 12 March 2026 and 20 March 2026 and included Authorising Officers, applying officers, and members of the Information Governance Team. The sessions covered the legislative framework, authorisation processes, compliance requirements under the Regulation of Investigatory Powers (Scotland) Act 2000 (RIP(S)A), and associated Codes of Practice. Further training and awareness-raising sessions are planned as required to ensure continued compliance across the Council.</p>

<p>Please provide details of any training provided since your last inspection on RIP(S)A considerations when using the internet or social media as part of investigations / enforcement activity:</p>	<p>Since the last inspection, the Council has arranged training to ensure staff are aware of RIP(S)A requirements when using the internet, social media, or other open-source information as part of investigations or enforcement activity. This training was delivered by an external provider on 12 March 2026 and 20 March 2026 and included Authorising Officers, applying officers, and members of the Information Governance Team. The sessions covered the legislative framework, compliance requirements, and good practice guidance for the lawful use of online platforms in investigative contexts. Further sessions are planned as necessary to maintain awareness and compliance across the Council.</p>
---	--

Governance	
<p>Please provide details of how the use of the internet and social media is overseen / monitored / audited to mitigate the risk of inadvertent, unauthorised RIP(S)A activity:</p>	<p>To mitigate the risk of inadvertent or unauthorised RIP(S)A activity, the Council has undertaken an exercise whereby the Information Governance Team gathered information from services regarding their use of social media and internet surveillance. A monitoring form has been developed to capture and assess this activity to ensure ongoing oversight of internet and social media use in investigations. The form and associated process are scheduled for review and approval through the Council's governance structure, including the Data Management and Compliance Group, the Data Governance Board, and final consideration by the Policy and Strategy Committee. This approach ensures regular monitoring, accountability, and alignment with RIP(S)A requirements.</p>
<p>Please provide details of your approach to the retention, review and destruction of any material obtained through covert powers and to demonstrate compliance with the Safeguards in Chapter 9 of the relevant Codes of Practice:</p>	<p>The Council maintains a structured approach to the retention, review, and destruction of material obtained through the use of covert powers to ensure compliance with the safeguards set out in Chapter 9 of the relevant Codes of Practice.</p> <ul style="list-style-type: none"> Operational Records and RIP(S)A Authorisation Forms: Retention periods are calculated from the date of cancellation or disposal of the authorisation, or when material is no longer required for prosecution or ongoing investigation. Records are reviewed

periodically, with destruction carried out when retention is no longer necessary. The standard retention period for review purposes is five years, in accordance with the Regulation of Investigatory Powers (Scotland) Act 2000, the Regulation of Investigatory Powers Act 2000, and the Covert Surveillance and Property Interference Code of Practice.

- CCTV and Routine Surveillance Records: For material obtained from routine CCTV recordings that are not required for prosecution or operational purposes, retention is triggered from the date of recording. Such recordings, including master copies of RIP(S)A authorisation forms where applicable, are destroyed or overwritten after seven days in line with statutory guidance.

This approach ensures that all material is appropriately safeguarded, regularly reviewed, and securely destroyed when no longer required, providing assurance of compliance with statutory obligations and internal governance requirements.

IPCO

Authorisation & Oversight

PO Box 29105, London
SW1V 1ZU

Mr Des Murray
Chief Executive
North Lanarkshire Council
PO Box 14
Civic Centre
Motherwell
ML1 1TW

08 April 2026

Dear Chief Executive,

Thank you for providing IPCO with your response to the matters identified in my Inspector's letter dated 12 January 2026.

I am satisfied that your reply provides assurance that ongoing compliance with RIP(S)A 2000 and the Investigatory Powers Act 2016 will be maintained. As such, your Council will not require further inspection this year. I am grateful for the assistance provided by your Chief Officer, Ms Blair, to my Inspector.

My Inspector notes that, while records meet the statutory requirements, compliance with the Codes of Practice would be strengthened if applicants and authorising officers addressed proportionality points as set out in the relevant Codes of Practice (Surveillance Code, paragraph 4.7; CHIS Code, paragraph 3.5). It may be helpful to reflect this in your revised policy at sections 1.8 and 2.9 respectively, noting the subtle differences between surveillance and CHIS requirements.

You have advised that your social media and online investigations processes are currently under review. This is timely, and you are encouraged to ensure that there is a robust monitoring process in place across all relevant departments within the Council.

As a relatively active user of surveillance powers, it is important that your policy remains fit for purpose and that elected members are afforded the opportunity to review RIP(S)A use at least once a year. While this is not mandated, rather it is advised within the Codes of Practice (paragraph 4.42), it strengthens the legitimacy of the use of these tactics.

I would ask that you ensure the key compliance issues continue to receive the necessary internal governance and oversight through you and your Senior Responsible Officer: ongoing training and awareness-raising; internal compliance monitoring by lead managers within their business areas; and the retention, review and destruction (RRD) of any product obtained through the use of covert powers (records and product management in accordance with the safeguards chapters of the relevant Codes of Practice).

Your Council will be due its next inspection in 2029, but please do not hesitate to contact my Office if IPCO can be of assistance in the intervening period.

It is, of course, the responsibility of your authority to ensure that any covert activity is conducted in accordance with the legislation. IPCO expects early notification of any errors in the use of these powers, which will then be investigated fully.

Yours sincerely,

Brian Leveson



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

Freedom of Information (Scotland) Act (FOISA)

IPCO is not a "public authority" for the purpose of FOISA and therefore falls outside its reach. Public authorities who are subject to these Acts may receive requests for disclosure of our reports. In the first instance the SRO should bring the matter to the IPCO Data Protection Officer (at: info@ipco.org.uk), before making any disclosure.