MIDLOTHIAN COUNCIL

COVERT SURVEILLANCE POLICY AND GUIDANCE

Document Control Information

Revision	Date	Revision Description
Version 1.0	19/5/16	
Version 2.0	26/3/2019	Updated to reflect recommendations from IPCO inspection December 2018
Version 3.0	23/06/2020	Updated to reflect correspondence from IPCO and changes in Council management structure
Version 4.0	18/01/2023	Updated to reflect comments from ICPO and appoint new Authorising Officer

	INDEX	Page

1. INTRODUCTION

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

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.

No activity shall be undertaken by employees of Midlothian Council that comes within the definition of "Intrusive Surveillance." Intrusive surveillance is detailed in Section 5 of this policy.

2. OBJECTIVE

The objective of this policy is to ensure that all covert surveillance by Midlothian Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Scottish Government's Covert Surveillance and Property Interference: Code of Practice 2017 and the 2021 Procedures and Guidance issued by the Office of Surveillance Commissioners (OSC). Copies of the Code of Practice and the Procedures and Guidance are available to all staff involved in surveillance operations and are available via the Midlothian Council Intranet.

The Code of Practice and the Procedures and Guidance can be accessed through the links below and all staff working in covert surveillance are expected to be familiar with these documents:

https://www.gov.scot/publications/covert-surveillance-property-interference-code-practice-2/

https://ipco-wpmedia-prod-s3.s3.eu-west-2.amazonaws.com/OSC-PROCEDURES-AND-GUIDANCE.pdf

If the procedures outlined in this policy are not followed, any evidence acquired may have been acquired unlawfully. It may therefore not be admissible in court, and the Procurator Fiscal is unlikely to take proceedings on the basis of such evidence. Midlothian Council may also be exposed to legal action.

3. SCOPE OF THE POLICY

This policy applies in all cases where "directed surveillance" is being planned or carried out. Directed surveillance is defined in the relevant Code of Practice as undertaken "for the purposes of a specific investigation or operation" and "in such a manner as is likely to result in the obtaining of private information about a person". This may also include repeated and systematic viewings of a subject's social media sites.

The policy does not apply to:

- Observations that are carried out overtly;
- Unplanned observations made as an immediate response to events where it was not reasonably practicable to obtain authorisation;
- Non-planned, ad hoc covert observations that do not involve the systematic surveillance for a specific investigation or operation; or
- Any disciplinary investigation or any activity involving the surveillance of employees of the Council, unless such surveillance directly relates to a regulatory function of the Council.

Unless the situation very clearly falls within one of these exempted categories, the authorisation procedures below should be followed in every case.

4. PRINCIPLES OF SURVEILLANCE

In planning and carrying out covert surveillance, Midlothian Council employees shall comply with the following principles:-

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

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

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

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

Effectiveness – planned covert surveillance shall be undertaken only by, or under the supervision of, suitably trained or experienced employees.

Proportionality – the use and extent of covert surveillance shall be proportionate and not excessive i.e. its use shall be in proportion to the significance of the matter being investigated. 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.

Collateral intrusion – Consideration must be given to the extent to which the surveillance will interfere with the privacy of persons other than the subject of the surveillance and to minimise the impact of the surveillance on them. Reasonable steps shall be taken to minimise the acquisition of information that is not directly necessary for the purposes of the investigation or operation being carried out.

Authorisation – all directed surveillance must be authorised in accordance with the procedures described below.

5. WHEN IS AUTHORISATION REQUIRED?

Seeking Authorisation

Authorisation is required for directed surveillance as defined in section 3 above.

Authorisation is required when the activity is carried out by Midlothian Council employees or by third parties carrying out surveillance on behalf of or under the instruction of the Council.

Where surveillance is to be undertaken in a manner likely to acquire “private information” about a person or persons (which is not defined but includes information about their private and family life) and is to be conducted in such a manner as is calculated to ensure the persons subject to the surveillance are unaware that it is or may be taking place, then authorisation will be required.

In some noise monitoring cases, where only the level of noise is recorded, an authorisation may not be necessary, further advice and guidance should be sought in such cases.

When directed surveillance has been carried out without the necessary authorisation, this must be reported to the Chief Surveillance Commissioner. In these circumstances, you should contact the Legal and Governance Manager.

More detailed advice and examples of when authorisation is required can be found in the Code of Practice and Procedures and Guidance.

Further advice as to whether an authorisation is required may be obtained via the Legal and Governance Manager.

WHO MAY SEEK AUTHORISATION?

Any officer whose duties involve activity falling within the above description must seek and be granted authorisation prior to carrying out the surveillance.

INTRUSIVE SURVEILLANCE

Intrusive surveillance means covert surveillance in relation to anything taking place on any residential premises (i.e. a person's accommodation) or in any private vehicle and involves the presence of an individual on the premises or in the vehicle or is carried out by means of a surveillance device. Midlothian Council is not authorised to conduct intrusive surveillance under any circumstances.

Some additional points should be made about intrusive surveillance. Surveillance is not intrusive if directed into a home or private vehicle from outside unless the information is consistently of the same quality as the device actually present in the home or vehicle would provide. Advice previously received from the OSC suggests that the sort of surveillance undertaken by the Council is unlikely to reach this level of sophistication. Thus activities such as filming goods being sold from the back of a car, or monitoring the level of noise generated by an anti-social tenant (but not the actual words) are unlikely to be classed as intrusive, and so these activities can safely be carried out (subject to appropriate authorisation).

6. WHEN IS COVERT SURVEILLANCE APPROPRIATE?

By its nature covert surveillance intrudes on people's privacy. It should therefore be regarded as a last resort, only to be considered when all other methods have been tried and failed, or where the nature of the activity the surveillance relates to is such that it can reasonably be concluded that nothing else will be able to acquire the information being sought.

Any use of covert surveillance must be proportionate to the objective being pursued.

7. PROPORTIONALITY

Proportionality is a concept of human rights law designed to ensure that measures taken by the State (and its organs such as the Council) which impact on the rights of citizens are kept within proper bounds. It means that if the same legitimate end can be reached by means of less intrusion on people's rights then the less intrusive path should be taken. There should also be a reasonable relationship between the seriousness of the mischief being addressed and the degree of intrusion into people's rights.

Covert surveillance involves a potentially serious breach of an individual's rights to privacy. Compelling reasons are therefore required to justify these, particularly if the surveillance is to continue for an extended period.

It is useful to consider how serious the breach you are seeking to rectify is. For criminal offences the potential sentence may be a useful guide. However many regulatory offences, while attracting only small fines, are designed to prevent potentially life threatening occurrences. Such factors weigh in favour of surveillance being proportionate.

8. CONFIDENTIAL INFORMATION

Applications where a significant risk of acquiring confidential information has been identified shall always require the approval of the Chief Executive only.

"Confidential Information" consists of:

- Matters subject to legal privilege (for example between professional legal adviser and client);
- Confidential personal information (for example relating to a person's physical or mental health); or
- Confidential journalistic information.

Such applications shall only be granted in exceptional circumstances where the authorising officer is fully satisfied that surveillance is both necessary and proportionate in these circumstances.

If the authorisation sought recognises the likelihood of acquiring Confidential Information, the Council's Legal and Governance Manager should be consulted for legal advice regarding whether the desired surveillance is reasonable and proportionate.

When any confidential information is obtained then the matter must be reported to the Investigatory Powers Commissioner's Office (IPCO) during their next inspection and any information obtained made available to them if required.

Confidential information must be destroyed as soon as it is no longer necessary to retain it for a specified purpose.

9. COLLATERAL INTRUSION

"Collateral Intrusion" refers to the fact that surveillance operations will often inadvertently intrude on the privacy of persons other than those at whom the operation is directed. Operations should be planned so as to minimise or eliminate so far as possible the risk of collateral intrusion, and the extent to which it remains is a factor to consider in determining the proportionality of the operation.

Collateral intrusion generally will be minimised through proper planning and by focussing the surveillance as much as possible on the specific person or premises targeted.

It is important to note that only the person(s) specified in the Directed Surveillance authorisation are subject to surveillance. Therefore, any records kept of the surveillance activity, i.e. notes; photos or video images should only contain details of person(s) specified. This should also be mentioned in the application to minimise collateral intrusion.

10. SURVEILLANCE BY OTHER PUBLIC AUTHORITIES

Council officers are occasionally asked to assist in surveillance operations being conducted by other public authorities, for example the Police, the Department for Work and Pensions, HM Revenue and Customs etc. In such cases it is for the organisation seeking assistance from the Council to ensure that it has appropriate authorisations in place. These authorisations should be shown to the Council staff involved or written confirmation given that the authorisations have been duly granted. Copies of such authorisations or written confirmations (from a proper officer of the other authority) should be forwarded to the Council's Legal and Governance Manager.

Where possible, the Council should seek to avoid duplication of authorisation as part of a single investigation or operation. Where two authorities are conducting directed or intrusive surveillance as part of a joint operation, only one authorisation is required.

11. CCTV

The Council has developed a Code of Practice to cover the operation and management of the Council's CCTV systems. This Code of Practice should be followed at all times but officers should be aware that formal authorisation will still be required under RIPSA if the system is to be used in Directed Surveillance operations.

Completion, Granting and Recording Authorisations and Refusals

Construction of Applications:

12. UNIQUE REFERENCE NUMBER (URN)

Prior to completion of a Directed Surveillance Application, a URN must be sought from the Legal and Governance Manager. Contact should be made with the Legal and Governance Manager advising that:

- A URN is sought,
- The name of the person subject to surveillance,
- Name of Applicant seeking authorisation.

The Legal and Governance Manager shall enter the URN on the central record and place a note on the record that an application is pending. This will

ensure that the Legal and Governance Manager will be aware of forthcoming application for the central record.

13. APPLICATION FORMS

Directed Surveillance Application – RIPSA1 (Appendix 1)

This application should be completed in all cases (including where oral authorisation was first sought). It is effective from the time that approval is given. When granting authorisations, Authorising Officers should indicate the frequency of reviews they consider necessary and specify the first review date, normally within one month. By law, an authorisation lasts for 3 months.

Directed Surveillance Review – RIPSA2 (Appendix 2)

This application should be completed in cases that require to be reviewed in accordance with the authorising officer's comments.

Directed Surveillance Renewal – RIPSA3 (Appendix 3)

The renewal application needs to be completed if the 3 month authorisation is due to expire and surveillance is still necessary and proportionate.

Directed Surveillance Cancellation – RIPSA4 (Appendix 4)

A cancellation form needs to be completed when it is clear that the authorisation is no longer required. An authorisation should not be allowed merely to expire after 3 months but must be formally cancelled.

14. WHO MAY GRANT/REVIEW/RENEW AND CANCEL AUTHORISATIONS?

Authorisations for directed surveillance may only be granted/reviewed/ renewed and cancelled by:-

- the Chief Executive;
- Executive Director, Place;
- Executive Director, Children, Young People and Partnerships;
- Chief Officer, Place; or
- the Legal and Governance Manager.

.

Applications where a significant risk of acquiring confidential information has been identified should only be granted by the Chief Executive, please refer to section 8 above.

Good practice dictates that the officer authorising surveillance is not operationally involved in the matter being authorised, although this may not always be practicable.

The Executive Director, Place has been appointed as the Council's Senior Responsible Officer. As such, it is also good practice that the Senior Responsible Officer does not grant authorisations but he is competent to do so if other Authorising Officers are not available.

15. URGENT AUTHORISATIONS

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

An urgent authorisation should not be used to remedy mere delay or failure to seek written authorisation timeously.

Urgent authorisations last for no more than 72 hours.

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

16. GRANT OR REFUSAL OF AUTHORISATIONS

All Divisions carrying out surveillance activities must maintain a record of all applications for directed surveillance, together with the relevant consent or refusal. Oral authorisation must be recorded on the appropriate form (RIPSA1) and submitted to the Authorising Officer. All applications, reviews, renewals and cancellations must be prepared and a copy delivered within 24 hours to the Legal and Governance Manager, Midlothian House, as the person responsible for the maintenance of the Central Record of Authorisations. These forms may be monitored for cross-service consistency by the Legal and Governance Manager, and may have to be produced in the event of an inspection by the IPCO. These forms represent evidence of the Council's compliance with the law and Codes of Practice, and as such, care should be taken in the completion and logging of them.

The IPCO may require an Authorising Officer to justify his decision to grant a request, so authorisations should not be signed off automatically. Evidence of reasoned grant or refusal of requests is vital in displaying compliance with the law.

The Authorising Officer must be satisfied that the Applicant has correctly identified a lawful purpose for the proposed surveillance, has planned the operation properly so as to minimise collateral intrusion and the collection of confidential information, is not proposing to stray beyond the permissible

bounds of directed surveillance, and has correctly applied the necessity and proportionality tests. Only if actively satisfied on these points should the authorisation be granted. Any restrictions imposed on the authorisation should be noted as Authorising Officer comments.

An authorisation should demonstrate how an Authorising Officer has reached the conclusion that the activity was proportionate to what it seeks to achieve, including an explanation of the reasons why the chosen method is not disproportionate.

The Authorising Officer should set out, in their own words, why they are satisfied or why they believe the activity is necessary and proportionate. A bare assertion is insufficient.

The Authorising Officer should as a matter of routine state explicitly and in their own words what is being authorised, and against which subjects, property or location (ie who, what, where, when and how). Mere reference to the terms of the application is inadequate.

Unless the request is straightforward or already includes clear information and sufficient level of detail to explain and justify the required activity, the Authorising Officer should seek clarification directly from the Applicant (face-to-face, by telephone or otherwise as appropriate), or from the Applicant's line manager on questions of policy. If still dissatisfied, the Authorising Officer should refuse the request or grant it subject to conditions or restrictions. Authorising Officers should make it clear, from the terms of their authorisations and comments, exactly what is being authorised, including any parameters or restrictions they are setting. Even if fully satisfied and accepting that there is no need to impose any restrictions, the Authorising Officers should make some comments in the 'Comments' box, perhaps confirming that they have discussed the matter with the Applicant (if appropriate) and that they are satisfied that the proposed operation is necessary and proportionate.

A copy of the authorisation should be passed immediately to the Applicant by the Authorising Officer or, if the request has been presented by someone else on the Applicant's behalf, eg the Applicant's line manager, that person should immediately forward the authorisation to the Applicant. Except in cases of urgency, Applicants should have sight of the written authorisation before commencing the activity, so they can satisfy themselves that full authorisation has been granted or acquaint themselves with any restrictions set by the Authorising Officer.

17. DURATION, REVIEW, RENEWAL AND CANCELLATION OF AUTHORISATIONS

By law an authorisation lasts for three months. If the reasons justifying carrying out the surveillance cease to apply, then the authorisation should be cancelled as soon as it is no longer required and a record kept of the cancellation and the reasons for this.

If surveillance is to be continued for longer than the original period authorised, it is necessary to have a renewal application authorised. Renewal applications should highlight the fact that what is sought is renewal, and enclose the original authorisation and any previous renewals. The tests applicable to renewals are identical to those for initial applications.

When granting authorisations, Authorising Officers should indicate the frequency of reviews they consider necessary and specify the first review date, normally within one month. Applicants should complete and submit a review form to the Authorising Officer in advance of each review date. The review form should note whether any significant evidence has been acquired by the activity being considered and whether, against the background, continued surveillance can still be justified.

18. SECURITY AND RETENTION OF DOCUMENTS

Documents created under this procedure are highly confidential and shall be treated as such. Divisions shall make proper arrangements for their retention, secure storage and destruction, in accordance with the requirements of the Data Protection Act 2018, the OSC Procedure and Guidance and the Code of Practice. The Legal and Governance Manager should also be advised of these arrangements. 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 (longer if required for ongoing criminal proceedings).

Paper copies of all documents must be stored in locked and secure filing cabinets. All electronic correspondence regarding an investigation must be stored in a secure directory which is not available outwith the immediate staff involved.

In accordance with the OSC Procedure and Guidance, documents will be inspected periodically by the Chief Executive to ensure that a consistent approach is being adopted by different Council Divisions. The IPCO have statutory powers of inspection and all records (applications, authorisations, and refusals) must be available for inspection. No records should be destroyed until after an IPCO inspection has had the opportunity to see them.

All documentation should be retained and destroyed in terms of the Council's data retention policy.

19. OVERSIGHT

Internal oversight is provided by the Council's Senior Responsible Officer. The Senior Responsible Officer is a member of the Corporate Management Team and is responsible for the integrity of the internal processes within Midlothian Council for the management of Covert Surveillance and for Council compliance with RIPSA and the Code of Conduct.

The Investigatory Powers Commissioner's Office (IPCO) provides independent oversight of the use of the powers contained within the Regulation of Investigatory Powers Act 2000 and Regulation of Investigatory Powers (Scotland) Act 2000. This oversight includes inspection visits by Inspectors appointed by the IPCO.

20. COMPLAINTS

The Regulation of Investigatory Powers Act 2000 (the 'UK Act') establishes 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 Regulation of Investigatory Powers (Scotland) Act 2000. Details of the relevant complaint procedure can be obtained from the Investigatory Powers Tribunal, PO Box 33220, London, SW1H 9ZQ.

21. REVIEW

This Policy should be reviewed as and when necessary to reflect any changes in circumstances and no later than every three years

APPENDICES

Directed Surveillance Application Form	-	Appendix 1
Directed Surveillance Review Form	-	Appendix 2
Directed Surveillance Renewal Form	-	Appendix 3
Directed Surveillance Cancellation Form	-	Appendix 4

These forms can be accessed on the Intranet via Council/Legal/Surveillance Guidance.