MIDLOTHIAN COUNCIL

POLICY AND GUIDELINES ON SURVEILLANCE THROUGH SOCIAL MEDIA

Document Control Information

Revision	Date	Revision Description
Version 1.0	19/5/16	
Version 2.0	08/08/2016	Updated to reflect recommendations from ICPO inspection June 2016
Version 3.0	26/3/2019	3 yearly review
Version 4.0	18/01/2023	3 Yearly review
Version 4.0	07/03/2024	Policy name change to 'Policy and Guidelines on Surveillance through Social Media'

	INDEX	Page

POLICY AND GUIDELINES ON SURVEILLANCE THROUGH SOCIAL MEDIA

See also separate Policy and Guidelines on Covert Surveillance

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").

This document sets out Midlothian Council's policy regarding internet surveillance using Social Media.

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.

In some circumstances, it may be necessary for Midlothian Council employees, in the course of their duties, to access social media websites either by creating covert identities or through the officer's departmental identity.

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.

There are ever increasing and changing types of social media eg Facebook, Instagram, TikTok etc. This guidance refers below to Facebook but the principles involved should be applied to dealings with any social media platform

2. OBJECTIVE

The objective of this policy is to ensure that all surveillance through social media conducted by Midlothian Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with Midlothian Council's RIPSA Policy, the relevant legislation, the Scottish Government's Code of Practice on Covert Surveillance ('the Code of Practice') and the Procedures and Guidance issued by the Office of Surveillance Commissioners.

The Code of Practice and the Procedures and Guidance can be accessed through the links below and staff 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 includes 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 outlined in the RIPSA Policy should be followed in every case.

4. MIDLOTHIAN COUNCIL SOCIAL MEDIA PRESENCE

Midlothian Council has an internet presence as a corporate entity as well as different services and departments. The corporate entity currently has a Facebook page and a twitter account. Access to these is limited to the Communications Team. Other services also utilise their respective corporate accounts to post information about the Council's activities and events. Also, individual schools have social media presence.

5. TYPES OF 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 department's representative; and
- Through a covert identity using a false name.

Officers must not use a private social media account whilst carrying out an investigation on behalf of the Council. Where there is a compelling operational requirement for Council Officers to conduct open source research using social media profiles then, once authorised by the relevant Executive Director or Senior Reporting Officer, Council facilities will be provided to enable the task to take place.

Investigators utilise social media in two different ways:

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

5.1 Privacy Settings of Account under Investigation

Most social media websites will have a variety of privacy settings that users can apply to protect their accounts from others accessing the information contained therein. Facebook is a social media website commonly used to investigate service users or potential service users and it has several different privacy settings. Therefore, Facebook will be used as an example in this policy. Depending on what privacy setting a user chooses, different people can access the account and see all or some of its contents.

'Public': All Facebook users can see the account and all of 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 and geographic location of the user.

'Friends': Only those who 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 ones for investigating officers are 'public' and 'friends', as option 3 is a sub-category of 'friends'.

5.2 Utilisation of Social media

Directed Surveillance using overt Council identity
If an investigating officer views a service User's Facebook profile, with whom they are not 'Friends' via a normal route, 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. An ad hoc or one off viewing/visiting of this profile will be overt and no authorisation under RIPSA will be required.

Whilst data may be considered "open source" where privacy settings are available but not applied, if the officer frequently or regularly views/visits the same individual's profile this must be considered as targeted and may constitute directed surveillance. Such actions must be considered on a case by case basis and where appropriate, authorisation under RIPSA 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 he is contacting them in his role as an employee of Midlothian Council, then this contact will be overt and no authorisation under RIPSA will be required. In any other instance, where the contact is not overt, authorisation for the use and conduct of a CHIS will be necessary.

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

Surveillance using covert identity
If an investigating officer befriends a service user under a covert identity, then a CHIS authorisation will always need to be in place before that is done.

The Council has developed Policy and Guidance on the use of Covert Human Intelligence Sources which is available on the intranet.

6. BEST PRACTICE 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 sites, an appropriate RIPSA authorisation should be completed.

7. AUTHORISATION

Please refer to Midlothian Council's Regulation of Investigatory Powers (Scotland) Act and the Covert Surveillance and Use of Covert Human Intelligence Sources Policies and Guidelines.

8. REVIEW

This policy will be reviewed every three years from the date of approval.

Further information on these guidelines and advice on whether a Directed Surveillance or CHIS authorisation is required may be obtained from the Legal and Governance Manager.