ORKNEY
ISLANDS COUNCIL

Surveillance through Social Media Policy

Contents

1. Introduction 3
2. Statement of Intent 3
3. Objective 3
4. Orkney Islands Council's Social Media Presence 3
5. Types of Investigators' Accounts 4
6. Types of Surveillance 4
7. Privacy Settings of Account under Investigation 4
8. Utilisation of Social Media 5
9. Best practice for the use of social media in investigations 6
10. Authorisation for all types of surveillance 6
11. Review of Policy 6

1. Introduction

1.1.

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

1.2.

Reference is made to Orkney Islands Council's policies and procedures in respect of covert surveillance and use of covert human intelligence sources (hereinafter collectively referred to as 'the Council's RIPSA policies and procedures'), to which this policy is subsidiary.

1.3.

In some circumstances, it may be necessary for Orkney Islands 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.

2. Statement of Intent

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.

3. Objective

The objective of this policy is to ensure that all surveillance through social media conducted by Orkney Islands Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the Council's RIPSA policies and procedures, the relevant legislation, the Scottish Government's Codes of Practice on Covert Surveillance and Property Interference and on Covert Human Intelligence Sources ('the Codes of Practice') and any guidance which the Investigatory Powers Commission may issue from time to time.

4. Orkney Islands Council's Social Media Presence

The Council has four main social media accounts. The OIC Updates Facebook page and Orkney Council Twitter feed are managed by the communications team and provide information about a range of Council activities. The OIC School Transport Facebook page is managed by the Education Service. The OIC Roads Twitter Feed is managed by the Council's roads team and provides updates about road conditions on the Churchill Barriers during adverse weather.

In addition, a number of services manage Facebook and Twitter accounts including primary and secondary schools, the museum service, the library and St Magnus Cathedral.

5. Types of Investigators' Accounts

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, or
- Through a covert identity using a false name.

6. Types of Surveillance

Investigators utilise social media in two different ways:

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

7. Privacy Settings of Account under Investigation

7.1.

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 would be the social media website that would be most commonly used by Orkney Islands Council Officers 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.

7.1.1. '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 or geographic location of the user.

7.1.2. 'Friends'

Only those whom the user has accepted as Facebook 'friends' are able to see the entire content of the user's page.

7.1.3. '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'.

8. Utilisation of Social Media

8.1. Surveillance using identity as department's representative or departmental account

'Public' privacy setting

8.1.1.

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. Any viewing/visiting of this profile will be overt and no authorisation under RIPSA will be required.

8.1.2.

If the officer frequently or regularly views/visits the same individual's profile this must be considered as targeted. However if the service user posts publicly, they can have no expectation of privacy and will give everybody the right to view their posts at any time and as many times as that person wishes to. Therefore, strictly speaking, no authorisation under RIPSA for directed surveillance is required. However, as a matter of best practice, an appropriate RIPSA authorisation should be sought.

8.1.3.

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 OIC, then this contact will be overt and no authorisation under RIPSA will be required.

'Friends' privacy setting

8.1.4.

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 an Orkney Islands Council employee, then the action could not be classified as covert. No RIPSA authorisation would be needed.

8.1.5.

In either of the above privacy settings, although the officer has been given access to the account with the consent of the owner, the officer will still need to consider 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.

8.2. Surveillance using covert identity

8.2.1.

If an investigating officer establishes a relationship with a service user under a covert identity in order to obtain, provide access to, or disclose information, then a covert human intelligence source ('CHIS') authorisation will always need to be in place before that is done.

8.2.2.

However if a covert identity is presented but no steps are taken to form a relationship with the subject, 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 in itself amount to establishing a relationship. Equally, the use of electronic gestures such as "like" or "follow" in order to react to information posted by others online would not in itself constitute forming a relationship. Nonetheless, it should be borne in mind that entering a website or responding to such gestures may lead to further interaction with that user or other users. A CHIS authorisation should be obtained if it is intended to engage in such interaction to obtain, provide access to, or disclose information.

9. 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.

10. Authorisation for all types of surveillance

Please refer to Orkney Islands Council's Policies and Procedures on Covert Surveillance and Use of Covert Human Intelligence Sources.

11. Review of Policy

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