



Surveillance through Social Media Policy

Contents

1. Introduction.....	3
2. Statement of Intent	4
3. Objective.....	4
4. Orkney Islands Council's Social Media Presence.....	4
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.....	7
11. Review of Policy	7
Document control Sheet	8

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 RIPSAs 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.

1.4.

Directed online surveillance using an officer's private social media account should not be undertaken in any circumstances given the personal and operational security risks which such use would be liable to present.

1.5.

Officers are referred to paragraphs 3.11 to 3.16 of the Scottish Government's [Code of Practice on Covert Surveillance and Property Interference](#) (December 2017) and paragraphs 4.7 to 4.14 of the Scottish Government's [Code of Practice on Covert Human Intelligence Sources](#) (December 2017) which provide operational examples that would assist staff in recognising situations where RIPSAs are potentially engaged in their investigations.

1.6.

Whilst much of the work undertaken by social workers is not in pursuance of the prevention or detection of crime, and is not within the purview of RIPSAs, research conducted online in the interests of a child may still engage an individual's rights under Article 8 of the European Convention of Human Rights (right to respect for one's private and family life). This should be considered by staff prior to conducting any research online, being aware of their obligations in ensuring such Article 8 rights are not infringed by any online research conducted in child protection cases. Therefore, a protocol containing an auditable process has been developed for circumstances where online research is considered necessary in the interests of child protection. The process is similar to the procedure for seeking a RIPSAs authorisation as commended by the Investigatory Powers Tribunal. The Orkney Health and Social Care Partnership shall be responsible for ensuring that this process is observed and responsible for adherence to the Safeguards in relation to retention, review and destruction of material obtained in accordance with the Council's RIPSAs Data Safeguards Compliance Process.

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 RPSA 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 several social media accounts, covering authority-wide and individual service areas or establishments. There are four authority-wide channels – Facebook, X (formerly Twitter), LinkedIn and Instagram. These channels are managed by the Communications team and provide information about a range of Council activities.

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.
- 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.
- 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 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. If the viewing/visiting of this profile is not specifically targeted, such viewing/visiting will be overt and no authorisation under RIPSA will be required.

8.1.2.

Notwithstanding paragraph 8.1.1 above, directed online surveillance may be invoked even where a service user posts publicly. If the officer frequently or regularly views/visits the same individual's profile this must be considered as targeted, particularly where regular views/visits are likely to result in obtaining private information, irrespective of privacy settings. Whilst, strictly speaking, it may be argued that no authorisation under RIPSA for directed surveillance is required in respect of public posts, as a matter of best practice, an appropriate RIPSA authorisation should be sought in such circumstances.

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 Orkney Islands Council, 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 RIPSAs 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 RIPSAs 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 year from the date of approval.

Document control Sheet

Review / Approval History

Date	Name	Position	Version Approved
1 May 2018	Gavin Mitchell	Head of Legal Services	V1.2– approved at General Meeting of the Council
11 May 2020	Gavin Mitchell	Head of Legal Services	V1.3
5 May 2021	Gavin Mitchell	Head of Legal Services	V1.3
9 October 2023	Gavin Mitchell	Head of Legal and Governance	V1.4
7 October 2025	Gavin Mitchell	Head of Corporate Governance	V1.5
16 June 2026	Gavin Mitchell	Head of Corporate Governance	V1.6

Change Record Table

Date	Author	Version	Status	Reason
11 May 2020	Gavin Mitchell	V1.3	Final	Reflect observations contained in IPC Inspection Report
7 October 2025	Gavin Mitchell	V1.5	Final	Reflect observations contained in P&R Committee report on 23 September 2025 and subsequently ratified by Full Council on 7 October 2025.
16 June 2026	Gavin Mitchell	V1.6	Final	Reflect enhancement suggested by IPCO Inspector and outlined in P&R Committee report on 16 June 2026.