Appendix 2

ANGUS COUNCIL

Surveillance through Social Media Policy

Version:	V01
Author:	David Thompson
Owner:	Jackie Buchanan
Date of Approval:	27 October 2020
Approved by:	P & R Committee
Date issued:	27 October 2020
Review Period	Annually
Review Date	October 2022
Next review date:	October 2023

Amendment Form

Version	Date	Brief Summary of Changes	Author

Contents

1. Introduction

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

1.2 Reference is made to Angus Council's policies and procedures in respect of covert surveillance and the use of covert human intelligence sources in terms of the Regulation of Investigatory Powers (Scotland) Act 2000 ("RIP(S)A")(hereinafter collectively referred to as 'the council's RIP(S)A policies and procedures'), to which this policy is a subsidiary.

1.3 In some circumstances, it may be necessary for Angus Council employees, during their duties, to access social media websites either by creating covert identities or through the officer's service identity. Examples of this include:-

- Checking the social media accounts of absconded children/young people, where they are public, as part of efforts to trace them
- Tracing birth parents during court proceedings involving children
- As part of assessments, to ascertain the veracity of information provided by parents and others
- Checking social media accounts to ascertain if counterfeit goods are being offered for sale
- Checking social media accounts to ascertain if services are being offered in respect of activities that require to be licensed (e.g. the sale of alcohol)

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. Online surveillance (which is not directed surveillance) should not be undertaken under any circumstances using an officer's personal social media account.**

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)

- paragraphs 4.7 to 4.14 of the Scottish Government's Code of Practice on Covert Human Intelligence Sources (December 2017)

- Note 289 of the Procedures and Guidance produced by the Office of the Surveillance Commissioners dated July 2016

These provide guidance and operational examples that would assist staff in recognizing situations where RIP(S)A is potentially engaged in their investigations. Links to these Codes of Practice are published on the RIP(S)A page of the council's intranet.

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 RIP(S)A, research conducted online in the interests of a child or vulnerable adult 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 RIP(S)A authorisation as commended by the Investigatory Powers Tribunal.

2. Statement of Intent

2.1 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

3.1 The objective of this policy is to ensure that all surveillance through social media conducted by Angus Council employees is carried out effectively, while remaining in accordance with the law. It should be read in conjunction with the council's RIP(S)A 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 Commissioner's Office may issue from time to time.

4. Social Media Presence

4.1 The council has three corporate social media channels – Facebook, Twitter and Instagram which are managed by the communications team and provide information about a range of council activities.

4.2 Service social media accounts are on our website: https://www.angus.gov.uk/social_media_links

4.3 In addition, several schools and parent council's also have their own Facebook accounts

5. Types of Investigators' Accounts

5.1 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

6.1 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 used by Angus 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

8.1.1 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 RIP(S)A 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 RIP(S)A for directed surveillance is required. However, as a matter of best practice, an appropriate RIP(S)A 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 Angus Council, then this contact will be overt and no authorisation under RIP(S)A 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 Angus Council employee, then the action could not be classified as covert. No RIP(S)A 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

9.1 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 RIP(S)A authorisation should be completed.

10. Authorisation for all types of surveillance

10.1 Please refer to Angus Council's Policies and Procedures on Covert Surveillance and Use of Covert Human Intelligence Source which can be found on the Council's intranet site.