St.Helens Council

Social Media Investigations Procedure

Version: 1.2

Date: October 2018

Version Control

Date	Version	Comments
March 2015	1.0	Draft Procedure
July 2017	1.1	Draft Procedure Review
October 2018	1.2	Reviewed Procedure

Table of Contents

1 Introduction

1.1 Social Media is used by a significant number of people in their day-to-day lives and is a deeply embedded means of communication. As a result, Social Media has become a tool that can be used by public authorities for investigatory purposes.

1.2 The use of Social Media as an investigatory tool has been recognised in the Office of Surveillance Commissioners (OSC) Procedures and Guidance, which includes 'Covert Surveillance of Social Networking Sites'. The OSC was superseded in September 2017 by the Investigatory Powers Commissioners Office (IPCO), however the IPCO has yet to issue updated guidance.

1.3 Covert Surveillance is regulated under the Regulation of Investigatory Powers Act 2000 (RIPA).

1.4 The Home Office issued revised Codes of Practice in August 2018 for Covert Surveillance and Property Interference, and Covert Human Intelligence Sources (CHIS), which include guidance on the use of Social Media for investigatory purposes.

2 What is Social Media

2.1 Social Media is defined as 'websites and applications that enable users to create and share content or to participate in Social Networking'.

2.2 Social Media tools include, but are not limited to:

- Blogs/Microblogging
- Social Networking
- Collaboration networking media
- Social bookmarking
- Photo and video sharing
- RSS aggregation services
- Wikis

2.3 Social Networking is defined as 'the use of dedicated websites and applications to interact with other users or to find people with similar interests to one's own'.

3 Council Policy

3.1 This Procedure should be read in conjunction with the Social Media Policy, RIPA Policy Guidelines, and other relevant policies, procedures and guidance as contained within the Information Management Framework.

3.2 The Social Media Policy contained within the Information Management Framework covers the use of Social Media for business and personal use, responsibilities, and the use of Social Media for investigations.

3.3 The RIPA Policy Guidelines covers the use of directed surveillance and covert human intelligence sources.

4 Office of Surveillance Commissioners Guidance

4.1 Whilst data may be deemed published and no longer under the control of the author, it is unwise to regard it as 'open source' or publicly available; the author has a reasonable expectation of privacy if access controls are applied.

4.2 Where privacy settings are available but not applied the data may be considered 'open source', and an authorisation is not usually required. Repeat viewing of 'open source' sites may constitute directed surveillance on a case by case basis, and this should be borne in mind.

4.3 Authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority with the subject of the investigation (i.e. the activity is more than mere reading of the site's content).

4.4 It is considered inadvisable for a member of a public authority to set up a false identify for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

4.5 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation. Explicit consent of the person whose identity is used should be obtained, and consideration needs to be given to the protection of that person.

5 Home Office Codes of Practice

Covert Surveillance and Property Interference

5.1 Whilst a person may have a reduced expectation of privacy when in a public place, covert surveillance of that person's activities in public may still result in the obtaining of private information, and may require a directed surveillance authorisation. Surveillance of publicly accessible areas on the internet should be treated in a similar way, particularly when accessing information on social media websites.

5.2 Much of the information gathered from the internet can be accessed without the need for a directed surveillance authorisation. However, if the study of an individual's online presence becomes persistent, or where material obtained from any check is to be extracted and recorded and may engage privacy considerations, a directed surveillance authorisation may need to be considered.

5.3 There may be a reduced expectation of privacy where information relating to a person or group of people is made openly available, however the intention when making the information available was not for it to be used for covert purposes such as investigative activity.

5.4 Simple preliminary examination with a view to establishing whether the site or its contents are of interest is unlikely to interfere with a person's reasonably held expectation of privacy and therefore not likely to require a directed surveillance authorisation. However, where information is systematically collected and recorded about a particular person or group, RIPA should be considered.

Covert Human Intelligence Sources

5.5 When an internet profile is used to establish or maintain a relationship with a subject of interest for covert purposes in order to obtain or provide access to information, a CHIS authorisation is likely to be required.

5.6 Where a social media account requires a minimal 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. This level of interaction will not require a CHIS but may require a directed surveillance authorisation, for example requesting to join a closed group known to be administered by the subject of interest connected to a specific investigation. However, if there is to be further interaction, a CHIS authorisation should be obtained.

6 Conducting Investigations

6.1 Management approval must be obtained by Officers to use Social Media for investigation purposes, and evidence of approval must be retained on file.

6.2 Management approval must be obtained by Officers to set up Social Media / Network accounts using the @sthelens.gov.uk email account for investigations to be conducted.

6.3 Only management approved Social Media / Network accounts can be used to conduct investigations.

6.4 A record of all Social Media / Network accounts set up for the purpose of conducting investigations must be maintained.

6.5 The use of Social Media for the purpose of an investigation is only permitted during normal working hours, and in accordance with the Social Media Policy, i.e. investigations should not be conducted in an officer's own time outside of work, unless explicit approval is obtained in advance.

6.6 A record of usage of the Social Media / Network accounts must be maintained, including date and time of use, and purpose of use.

6.7 Management approval must be obtained to conduct an investigation into an individual using Social Media / Networks.

6.8 If it is deemed appropriate for an investigation to be undertaken in respect of an individual using Social Media, steps need to be taken to establish if the Social Media / Network account has had the privacy settings applied. If the privacy settings have been applied, the account cannot be considered an open source or publicly available and as such RIPA will apply.

6.9 If the privacy settings are available and have not been applied, the Social Media / Network account can be considered 'open source', and the account can be viewed. Repeat viewing may constitute directed surveillance, as such RIPA may apply, and this should be discussed with management.

6.10 The Terms and Conditions of the Social Media website being reviewed must be complied with at all times.

6.11 A record of all attempts to view individual Social Media / Networks must be maintained, including the name of the individual, date of access, Social Media / Network accounts accessed, purpose, privacy settings applied, information obtained, the officer conducting the investigation and the Social Media / Network account used.

6.12 Using third party data, i.e. family and friends of the individual, is not appropriate.

6.13 Any data obtained (i.e. screen prints) from viewing an individual's Social Media / Network account should be redacted for any third party data.

6.14 Officers must not attempt to engage with the individual or their family and friends.