Appendix 5

Using Social Media and Networking Sites in Investigations Policy

A. Introduction

1.0 Social Media has become a significant part of many people's lives. By its very nature, Social Media also often know as Social Networking sites can accumulate a sizable amount of information about a person's life. Their accessibility on mobile devices can also mean that a person's precise location at a given time may also be recorded whenever they interact with a form of Social Media on their devices. This means that incredibly detailed information can be obtained about a person and their activities.

1.2 Social Media can therefore be a very useful tool when investigating alleged offences with a view to bringing a prosecution in the courts. However, there is a danger that the use of Social Media can be abused, which would have an adverse effect damaging a potential prosecution and could even leave the Council open to complainants or criminal charges itself.

1.3 This Policy sets the framework on which the Council may utilise Social Media when conducting investigations into alleged offences. Whilst the use of Social Media to investigate is not automatically considered covert surveillance, its misuse when conducting investigations can mean that it crosses over into the realms of covert and or targeted surveillance, even when that misuse is inadvertent. It is therefore crucial that the provisions of the Regulation of Investigatory Powers Act 2000 (RIPA), as it relates to covert and directed surveillance, are followed at all times when using Social Media information in investigations.

1.4 It is possible for the Council's use of Social Media in investigating potential offences to cross over into becoming unauthorised surveillance, and in so doing, breach a person's right to privacy under Article 8 of the Human Rights Act. Even if surveillance without due authorisation in a particular instance is not illegal, if authorisation is not

obtained, the surveillance carried out will not have the protection that RIPA affords and may mean it is rendered inadmissible.

1.5 If is the aim of this Procedure to ensure that investigations involving the use of Social Media are done so lawfully and correctly so as not to interfere with any persons human rights but to ensure that evidence gathered from Social Media is captured and presented to court in the correct manner by obtaining the correct authorisations where necessary.

1.6 Officers who are involved in investigations, into both individuals and businesses they suspect to have committed an offence, should consult Legal Services if they are unsure about any part of this Policy and how it affects their investigative practices.

B. Regulation of Investigatory Powers Act 2000 (RIPA)

2.0 As there is an increase in the use of smartphones and other personal and portable devices, there is a significant amount of information on an individual's Social Media pages. This information might be relevant to an investigation being undertaken by the Council. However unguided and thought out research into a person's site could fall within the remit of RIPA and therefore require authorisation prior to it being undertaken.

2.1 Officers embarking on any form of investigatory action should always do so with RIPA in mind. Whilst RIPA will not always be relevant to every investigation, it is vital that enforcement officers and those involved in investigations regularly review their conduct with respect to investigatory actions. Any investigation is capable of evolving from one not requiring any RIPA authorisation to one that does at any point.

2.2 This Policy should be read in conjunction with the Council's current RIPA Policy and Procedures as well as statutory codes of practice issued by the secretary of state and the office of Surveillance Commissioners Guidance.

C. Definition of Social Media

3.0 Social Media also referred to as a Social Network can take many forms. Therefore, it is difficult to provide a definitive list of sites.

3.1 Current examples of popular forms of Social Media include (but the list is not exhaustive and new ones can be created whilst established ones popularity can wain).

Facebook	Twitter	Instagram
Linkedin	Pinterest	Reddit

3.2 Social Media will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile which contains personal information and is viewable by others, whether accepted as "friends" or otherwise.

3.3 The definition of 'private information' under the Regulation of Investigatory Powers Act (RIPA) includes:

"any information relating to a person's private or family life and should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships.'

D. Privacy Settings

4.0 The majority of Social Media services will allow its users to decide who can view their activity, and to what degree, through the use of privacy settings. Whilst some users are happy, or indifferent about who is able to view their information, others prefer to maintain a level of privacy.

4.1 Many users may purposely use Social Media with no privacy settings applied, this could be their intention as they are actively promoting something such as a business or event, and therefore require as many people as possible to be able to view their profile. Others may do so for reasons of self-promotion – this is known as a public profile and the information is "open source".

4.2 Persons operating Social Media without or with limited privacy setting do so at their own risk. Whilst the content or information shared by individuals on Social Media remains the property of that individual, it is nonetheless considered to be in the public domain. Publishing content or information using a public rather than a private setting means that person is allowing anyone to access that information however you have to proceed with care when accessing such accounts as although the privacy settings might allow you to enter them the information was not made available in this way for a covert purpose such as investigating and monitoring.

4.3 A private Profile is one set up on Social Media where the individual has set privacy settings and does not want their information open to public view, they will set the privacy setting appropriate to what they require.

4.4 By setting a private profile setting a user does not allow everyone to access their content and respect should be shown to that person's right to privacy under Article 8 of the Human Rights Act. This does not however extend to instances where a third party takes information and shares it on their own profile. So Person A has a private profile but a friend of theirs Person B takes something from Person A's page and shares it on their public page, this cannot be used from Person A's page but could from Person B's as they have a public profile.

E. Process to Follow when considering Using Social Media Sites

5.0 If an individual has a public profile an officer needs to be careful only to gather such information that is relevant to proving the offence they are investigating, if in any doubt seek advice from Legal Services. Even with Public profile sites care must be taken to

ensure that the correct authorisation is required if the monitoring of an account becomes planned and directed.

5.1 Officers must not use their own personal or private account when accessing social media sites for investigation and evidence gathering purposes. Only Council accounts should be used. Interaction and conversations of any kind should be avoided.

5.2 Officers should keep in mind that simply using profiles belonging to others, or indeed fake profiles, in order to carry out investigations does not provide them with any form of true anonymity. The location and identity of an officer carrying out a search can be easily traced through tracking of IP Addresses, and other electronic identifying markers.

5.3 One off visits or infrequent visits to an individual's Social Media profile spread over time cannot be considered "directed surveillance" for the purposes of RIPA, repeated or frequent visits may cross over into becoming "directed surveillance" requiring RIPA authorisation. A person's Social Media profile should not, be routinely monitored on a daily or weekly basis in search of updates, as this will require RIPA authorisation. If an officer requires more advice on this they should contact Legal Services.

5.4 Each viewing of a company or individual's social media profile for the purpose of investigation or evidence gathering must be recorded on the case log.

5.5 See paragraphs 4.11 to 4.17 of the Covert Human Intelligence Source Code of Guidance (August 2018)
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf

5.6 See Paragraphs 3.10 to 3.17 of the Covert Surveillance and Property Interference revised code of practise
https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

F. Capturing Evidence

6.0 Evidence that is of a readable form, ie text, status updates or photographs should be copied directly from the site or captured via a screenshot, onto a hard drive or some other form of storage device and then subsequently printed to a hard copy. The hard copy of evidence should then be exhibited to a prepared witness statement in the normal way.

6.1 If evidence is an audio or video content then efforts should be made to download that content onto a hard drive or some other form of storage device such as CD or DVD. Those CD's and/or DVD's should then be exhibited to a suitably prepared witness statement in the normal way. If you have difficulties with this contact the Council's IT Unit.

6.2 Screen shots – should display the time and date in order to prove when the evidence was captured, without this information the effectiveness of the evidence is potentially lost as it may not be admissible in court.

6.3 When capturing evidence from a Social Media profile steps should be taken to minimise the collateral damage of inadvertently capturing innocent third parties information. This might be particularly prevalent on Social Media profiles promoting events

G. Retention and Destruction of Information obtained

7.0 Where recorded material (in any form or media) is obtained during the course of an investigation which might be relevant to that investigation, or another investigation, or to pending or future civil or criminal proceedings, then it should be retained in accordance with the Date Protection Act 2018, the Freedom of Information Act 2000 and any other legal requirements including the council's Information asset register and Council's retention schedule. Advice should be sought from the relevant officer at the Council. Contact the Council's Compliance Officer for details of how to log the details.

7.1 All information should be retained and destroyed in accordance with the time scales provided in the Councils retention Policy

H. Review

8.0 This Policy will be reviewed periodically and in line with the Council's RIPA Policy and Procedure (Section A, para 6) to ensure that both documents remain current and compliant with relevant legal requirements and best practice guidance.

Revised - 3.11.20