Guidance on the use of Social Networking Sites for Investigations/Gathering Evidence

1. Introduction

1.1 This Guidance sets out how the Council may utilise social networking sites when conducting investigations into alleged offences or in the discharge of other duties performed by the Council.

1.2 It is recognized that the use of the internet and, in particular, social networking sites such as Facebook, LinkedIn, Twitter, Snapchat, Instagram, and other internet sites such as E-Bay can provide useful information for Council staff carrying out investigations or gathering evidence when dealing with service users. However, accessing an individual's or company's internet and social networking sites may potentially fall within the definition of covert directed surveillance, which would require authorization to be sought froma Magistrates Court.

1.3 Failure to seek authorisation when necessary could result in the Council breaching an individual's right to privacy (Article 8 of the Human Rights Act). It is therefore important that officers adhere to the Council's policy in respect of The Regulation of Investigatory Powers Act ('RIPA Policy') and this guidance when considering accessing internet and social networking sites as part of an investigation or to gather evidence.

1.4 The aim is to ensure that information gathering, investigations or surveillance involving the use of social networking sites are conducted lawfully and correctly in accordance with an individual's human rights and with due consideration of relevant legislation including:

- the Human Rights Act 1998 (HRA);
- the Data Protection Legislation (the Data Protection Act 2018 (DPA) and the General Data Protection Regulation (GDPR) and
- the Regulation of Investigatory Powers Act 2000 (RIPA) together with the published codes of practice from the Home Office, Investigatory Powers Commissioner's Office (IPCO), and the Information Commissioner's Office.

1.5 Use of social media in investigations refers to any instance where an officer accesses social media as described to formally or informally gather evidence for any kind of investigation.

2. What is meant by 'social media' or 'social networking sites' for the purposes of this Guidance

2.1 Social media will always be a web-based service that allows individuals and/or businesses to construct a public or semi-public profile (also known as social network services or "SNS") and will often have some, or all, of the following characteristics;

2.1.1 the ability to show a list of other users with whom they share a connection; often termed "friends" or "followers",

2.1.2 the ability to view and browse their list of connections and those made by others within the system, and /or

2.1.3 hosting capabilities allowing users to post audio, photographs and/or video content that is viewable by others

2.2 It is not possible to provide a definitive list of social networking sites so this should be taken to mean any site which involves individuals creating a profile which contains personal/private information and is viewable by others, whether accepted as "friends" or otherwise. Some current examples of the most popular forms of social networking sites, and therefore the most likely to be of use when conducting investigations, include: Facebook, Twitter, Instagram, LinkedIn and YouTube.

2.3 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."

3. Privacy settings

3.1 The fact that digital investigation is routine or easy to conduct does not mean that relevant legislation should not be considered. Care must be taken to understand how the social networking site in question operates. Any officer using a social networking site for investigation must not be tempted to assume that one service provider is the same as another or that the services provided by a single provider are the same.

3.2 Whilst it is the responsibility of an individual to set privacy settings to protect unsolicited access to private information, and even though 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. In some cases data may be deemed private communication still in transmission (instant messages for example).

3.3 Council officers **should not** attempt to circumvent privacy settings and view an individual's information on multiple occasions unless authorisation has been sought under RIPA. Such attempts may include, but are not limited to;

- 3.3.1 sending "friend" or "follow" requests to the individual;
- 3.3.2 setting up or using bogus social media profiles in an attempt to gain access to the individual's private profile;
- 3.3.3 contacting the individual through any form of instant messaging or chat function requesting access or information;
- 3.3.4 asking family, friends, colleagues or any other third party to gain access on their behalf, or otherwise using the social media accounts of such people to gain access; and /or
- 3.3.5 using any other deceptive or misleading method

3.4 By setting their profile to private, a user does not allow everyone to access and use their content. This **does not**, however, extend to instances where a third party takes it upon themselves to share information which originated on a private profile on their own social media profile. For example:

*Person A publicises on their private social media page that they intend to throw a party, at which they will be selling alcohol and providing other forms of licensable activities, despite not having a licence from the Council to do so. Person B, who "follows" Person A's social media page, re-publishes this information on their public social media page. The information on Person A's profile **cannot** be used, however the same information on Person B's profile, can.*

3.5 Where privacy settings are available but not applied the data **may** be considered "open source" or publicly available (i.e. there is a reduced expectation of privacy). However in some circumstances privacy implications still apply. This is because the intention when making such information available was not for it to be used for a covert purpose such as investigative activity. This is regardless of whether the social media user has sought to protect such information by restricting its access by activating privacy settings. Multiple and systematic viewing of the information would therefore require a RIPA authorisation.

3.6 When the use of social media is allowed or not allowed:

What is allowed	**What is not allowed**
Using different social media/social networking platforms to gather information that is publicly available	Sending "friend" or "follow" requests, set up a profile in an attempt to gain access to the individual's private profile or ask family, friends, colleagues or any other third party to gain access without a RIPA authorisation
Using information posted on a public profile without RIPA Authorisation	Repeated and/or regular viewing (more than 2 or 3 times) of "open source" content without a RIPA authorisation
Using social media for surveillance with a RIPA authorisation where the investigation is unusual and/or is likely to capture confidential information and the risks to privacy have been assessed as being proportionate and justified	Making contact through social media without a CHIS authorisation

4. Regulation of Investigatory Powers Act 2000 (RIPA)

4.1 This guidance should be read in conjunction with the Council's Policy and Procedural Guidance: (RIPA)

4.2 RIPA issues do not normally arise at the start of any investigation which involves accessing "open source" or publicly available material but what may begin as a lawful overt investigation can drift into covert surveillance which falls into the legislation.

4.3 Repeat and/or regular viewing of publicly available social media sites as opposed to one-off viewing may constitute directed surveillance and require authorisation under RIPA/other legislation. A person's social media profile should not, for example, be regularly monitored without a RIPA authorisation. You should not view the information/source more than twice within a limited timeframe. If you feel further viewing is necessary for an investigation you should refer to the RIPA

Policy and Procedural Guidance. It is important to note that RIPA authorisations have to pass a serious crime threshold, i.e. there must be an offence which is being capable of being punished by imprisonment of six months or more.

4.4 Where an officer intends to engage with others online using a false identity and establish/maintain a relationship without disclosing his or her identity, a CHIS authorisation may be required.

5. General considerations

5.1 For those individuals/businesses who do have a public profile on social media, data posted can be viewed, recorded and possibly used as evidence e.g. photographs, video content, messages or status. Officers must not use their own personal or private account when accessing social networking sites for investigations/evidence gathering, only Council accounts should be used.

5.2 Only information that is relevant to the investigation at hand, and goes some way toward proving the offence, or issue, should be gathered. Information about third subjects should be kept to a minimum.

5.3 Please note that the location and identity of an officer carrying out a search can be easily traced and the profiles can be flagged as a 'suggested friend'.

5.4 Officers should evaluate findings objectively and ensure that they are sure of the source and can rely on the information obtained.

6. Record keeping

6.1 Where evidence takes the form of any readable or observable content, such as text, status updates or photographs, it is acceptable for this to be copied directly from the site, or captured via a screenshot and copied onto a relevant electronic system. If necessary audio or video content can be captured.

6.2 When capturing evidence from a public social media profile, steps should be taken to ensure that all relevant aspects of that evidence are recorded effectively. For example, the time, date and status update should be visible on the screenshots.

6.3 When capturing evidence from a social media profile, steps should be taken to minimise the risk of collecting third party personal or private details alongside that of the person under investigation/suspected offender, either before capturing the evidence, or subsequently through redaction.

6.4 Where relevant records are obtained during the course of an investigation they should not be destroyed but kept for as long as they are needed. They should be retained in accordance with the requirements of the Data Protection Legislation, the Freedom of Information Act 2000, Criminal Procedures and Investigations Act 1996 (i.e. consider using the evidence obtained in a sensitive unused material schedule) and any other legal requirements.