Guidance re Use of Social Media in Investigations

1. Introduction

1.1 This Guidance note sets out how the Council may utilise Social Media when conducting investigations into alleged offences or information gathering in the discharge of other duties performed by the Council.

1.2 The aim is to ensure that information gathering, investigations or surveillance involving the use of Social Media are conducted lawfully and correctly in accordance with an individual's human rights and with due consideration of relevant legislation together with the published codes of practice from the Home Office, Investigatory Powers Commissioner's Office (IPCO), formerly the Office of Surveillance Commissioners (OSC), and the Information Commissioner's Office.

1.3 Use of Social Media in investigations refers to any instance where an officer accesses Social Media as described to formally or informally gather information for any kind of investigation.

2. What is meant by 'Social Media'

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"). Some current examples of the most popular forms of Social Media include: Facebook, Twitter, Instagram, LinkedIn and YouTube.

3. Privacy Settings

3.1 If access controls are applied an author has a reasonable expectation of privacy. 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.

3.2 Open Source information is any publicly available information, including information responsive to Google or other search engine searches, information publicly available on social media such as twitter, Instagram, Facebook etc. Information which is only available because you are a 'friend' of the target, information subject to privacy controls on Facebook or other social media, private communications such as texts to someone else, WhatsApp messages, private emails, direct messages on twitter is not open source.

3.3 It is the responsibility of an individual to set privacy settings to protect unsolicited access to private information however it is unwise to regard it as "open source" or publicly available where access controls are applied even though data may be deemed published and no longer under the control of the author.

3.4 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.

4. **Regulation of Investigatory Powers Act 2000 (RIPA)**

4.1 This guidance should be read in conjunction with Bristol City Council's Regulation of Investigatory Powers Act 2000 Policy and Procedures (RIPA Procedural Guidance)

4.2 It is important to note that RIPA authorisations have to pass a serious crime threshold, ie there must be an offence which is being capable of being punished by imprisonment of six months or more. See below for guidance on use of social media outside RIPA

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

4.4 Repeat and/or regular viewing of publically available Social Media sites without the individuals consent as opposed to a one off viewing may constitute directed surveillance and require authorisation under RIPA. A person's Social Media profile should not, for example, be regularly monitored without their consent without a RIPA authorisation. If you feel further viewing is necessary for an investigation you should refer to the RIPA Procedural Guidance.

4.5 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. **Article 8 Human Rights Act 1998**

5.1 If the monitoring is not for the purposes of detecting or preventing serious crime but for another purpose, for example for a statutory safeguarding purpose, the monitoring is outside the ambit of RIPA.

5.2 A proper public interest purpose/ Article 8(2) justification and the necessity and proportionality of using a social networking site or conducting a test purchase from an online marketplace must always be must always be established and recorded (see below

5.3 Specific legal advice will be required in order to establish a lawful basis for covert direct surveillance and a court order may be required.

5.4 If appropriate consent in writing to monitoring or reviewing of private information

(including some open source information as above) is obtained the issue of privacy does not arise. The consent has to be informed and freely given and the person consenting must have capacity to consent and understand exactly what they are agreeing to. The subsequent monitoring/review and use of the data must not go any further than the agreement.

5.5 Should the Council be found to have acted unlawfully in gathering evidence, the court may rule that the evidence can be admitted BUT the Council could be ordered to pay significant compensation.

6. Record Keeping

6.1 If the investigation does not fall within the ambit of RIPA (eg in a child protection case), a specific record should be kept of the decision and rationale for it ie whether the interference with the subject's Article 8 rights is justified with reference to the provisions in Article 8.2 and why the interference is necessary and proportionate.The Non RIPA form is on the Source for this purpose

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. 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.

6.3 Only information that is relevant to the investigation at hand, and goes some way toward proving the offence, issue or safeguarding concern should be gathered.
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 and any other legal requirements.

7. General Considerations

7.1 Only Council accounts should be used, not officers' private accounts.

7.2 Please note, 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'.

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

8. What you must do.

- Read the Bristol City Councils RIPA procedural guidance
- Make sure you have the appropriate authorisation when needed BEFORE using social media
- If in doubt, seek advice

9. Review

This Policy will be reviewed annually to ensure that it remains current and compliant with relevant legal requirements and best practice guidance.