Appendix 3

Social Media Policy

It is important to be aware that the use of social media in an investigation could, depending on how it is used and the type of information that is likely to be obtained, constitute covert activity that requires authorisation under RIPA.

Generally, researching 'open source' material would not require authorisation. However, return visits to build up a profile could alter the position as it could constitute directed surveillance depending on the circumstances. 'Open source' materials are those that can be viewed on social media without becoming a subscriber, follower or friend.

The internet may be used to gather intelligence and/or as a surveillance tool. Where online monitoring or investigation is conducted covertly for the purpose of specific investigation or operation it is likely to result in obtaining private information about a person or group, an authorisation for directed surveillance should be considered. Where a person acting on behalf of a public authority is intending to engage with others without disclosing their identity, a Covert Human Intelligence Source (CHIS) authorisation may be required. (then 4.16)

Where an officer intends to access a social media or other online account where they have been given access with the consent of the owner, the Council will still need to consider whether the account may contain information about others who have not given their consent. If this is likely to include private information about others, a directed surveillance authorisation should be considered, especially where there is an intention to monitor the account.

Where an officer is required to register providing personal identifiers (such as a name or phone number) before access to the site, RIPA authorisation will not be required. Officers should not a false identity to disguise online activities. The use of a false identity should not be used for a covert purpose without authorisation.

A preliminary examination of social media to establish whether the site or its contents are of interest is unlikely to interfere with a person's reasonable expectation of privacy and is not likely to require a directed surveillance authorisation. However, if there is a systematic recording of information about a particular person or group, a directed surveillance authorisation is likely to be required.

Where general monitoring is being undertaken of the internet in circumstances where it is not part of a specific, ongoing investigation or operation to identify themes, trends or factors that may influence operational strategic will not require RIPA authorisations. If the activity leads to discovery of previously unknown subjects or interest, once it is decided to monitor those individuals as part of an ongoing operation or investigation authorisation should be considered.

To determine whether a directed surveillance authorisation should be sought for accessing information on a website as part of a covert investigation or operation, it is necessary to look at the intended purpose and scope of the online activity it is proposed to undertake. Factors that should be considered in establishing whether a directed surveillance authorisation is required include:

- Whether the investigation or research is directed towards an individual or organisation;
- Whether it is likely to result in obtaining private information about a person or group of people (eg names, telephone numbers ,and address details)
- Whether it is likely to involve visiting internet sites to build up an intelligence picture or profile
- Whether the information obtained will be recorded and retained;
- Whether the information is likely to provide an observer with a pattern of lifestyle;
- Whether the information is being combined with other sources of information or intelligence, which amounts to information relating to a person's private life;
- Whether the investigation or research is part of an ongoing piece of work involving repeated viewing of the subject(s);
- Whether it is likely to involve identifying and recording information about third parties, such as friends and family members of the subject of interest, or information posted by third parties, that may include private information and therefore constitute collateral intrusion into the privacy of these third parties.

To ensure that no unauthorised online covert surveillance takes place within the Council, please ensure that advice is sought from Legal Services

Recording Social Media Activity

Auditable records should be retained when activity is carried out on the internet in a way which staff may interact with others by using publicly open websites eg social networking services or private exchanges such as e.messaging sites, in circumstances where the other party may not reasonably be expected to know their true identity. Managers are expected to regularly review the internet activity of their teams and maintain records as they may be requested by the RIPA assessor . A template is attached.

To ensure that council resources are used in a controlled, auditable and manner please refer to the relevant Codes of Practice –

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742041/201800802_CSPI_code.pdf

https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/742042/20180802_CHIS_code_.pdf