DOVER DISTRICT COUNCIL

POLICY ON THE USE OF SOCIAL MEDIA IN INVESTIGATIONS OF CRIMINAL OFFENCES

November 2020

USE OF SOCIAL MEDIA IN INVESTIGATIONS OF CRIMINAL OFFENCES

POLICY

CONTENTS

Introduction

This Policy should be read alongside the Councils Regulation of Investigatory Powers Policy.

Scope

The policy applies to any Dover District Council employees that use social media for investigatory purposes and provides guidance to staff on the correct procedure.

Background

This policy is to ensure that employees know the procedures and process they must abide by when using social media for investigatory purposes and how they would go about doing so.

1 REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

1.1 This policy should be read in conjunction with the Dover District Council's RIPA Policy and Procedure, as well as the statutory codes of practice issued by the Secretary of State and the Office of Surveillance Commissioners Guidance.

1.2 It applies to any investigatory work undertaken by Dover District Council officers in relation to investigation and prosecution of criminal offences.

1.3 RIPA authorisation for the surveillance of social media makes the surveillance lawful for all purposes providing safeguards if, for example, a claim is made under Article 8 of the European Convention on Human Rights (right to respect for private and family life)

1.4 Social media has become a significant part of many people's lives, with people regularly using and interacting with many different forms of social media. For individuals to do so they are required to input numerous categories of personal data into sites before they can access the site. This is processed by the provider therefore they are accumulating a lot of personal data about a person, from daily routines to specific events. To create an account, most social media sites require at a minimum the name, username and email address of that individual. Further information may also be available in the profile itself.; Access to social media by a user on mobile devices can mean that a person's precise location at a given time may be recorded providing certain permissions are set.

1.5 Social media can therefore be a very useful tool when investigating alleged offences with a view to bringing a prosecution in the courts or taking other action. The use of information gathered from the various forms of social media available can go some way to proving or disproving various information including a statement made by a defendant, or an allegation made by a complainant.

1.6 Not all information published on social media is true and care must be taken as to the validity of information recorded. The information obtained must only relate to the investigation being carried out and not for a general "fishing" expedition.

2 'SOCIAL MEDIA' IN THIS POLICY

2.1 Social media encompasses a wide and dynamic range of web-based services typically facilitating individuals or businesses to construct a public or semi-public profile or creating a platform for sharing views or information. Typical characteristics include:

- The ability to show a list of other users with whom the primary user shares a connection, often termed "friends" or "followers"
- Hosting capabilities for audio, photographs and video content
- Community-based web sites/pages, online public discussion forums and chat rooms
- For sale pages embed in certain sites such as Facebook and Instagram

Current examples of social media include:

- Facebook
- Twitter

- Instagram
- Snapchat
- LinkedIn
- Pinterest
- Google+
- Vine
- Tumblr
- Flickr
- YouTube
- Reddit
- Yammer

2.2 This is not an exhaustive list and similar or new electronic communication systems are likely to be used when using social media for investigatory purposes.

3 PRIVACY SETTINGS

3.1 The majority of social media services will allow users to dictate who can view their activity, and to what degree, through the use of privacy settings. Depending on the social media site privacy settings this can just be limited to a user/display name.

3.2 The information publicly available is known as an individual's public profile.

3.3 Publishing content or information using a public, rather than a private setting, means that the individual publishing it is allowing everyone to access and use that information and to associate it with them. It should not be seen however as a consent to being monitored by the council unless done so in an overt manner. The information is still the personal data of that individual regardless of whether the information is made public.

3.4 The opposite of a public profile is a private profile, where a user does not allow everyone to access and use their content, and respect should be shown to that person's right to privacy under Article 8 of the European Convention on Human Rights. Even though an account is private certain aspects may still be visible depending on the site being used.

3.5 Even though a user has set their profile to private it may still be accessible through other means for example someone may have them as a friend linking them to that individual's social media profile which means their account isn't private to them; this may mean your friend can view their profile. Care should be taken and if there is any doubt about the use of any personal information it should be discussed with your line manager or data protection team.

4 THE PRINCIPLES

4.1 The diversity of social media means that it is impracticable to prescribe the threshold for requiring authorisation under RIPA in all of the various scenarios that may exist. Ultimately any decision to make an application should be taken

pragmatically and then actioned as per the relevant policies and procedures as referenced above. Covert surveillance should be the last measure.

4.2 Either authorisation for directed surveillance or for use of a Covert Human Intelligence Source (CHIS) may be required.

4.3 If in any doubt, the guiding principle is to refer to your line manager, with assistance from Corporate Services and the Solicitor to the Council, as necessary.

4.4 Reviewing open source sites does not require authorisation unless the review is carried out with some regularity.

4.5 Using social media for investigatory purposes, under statutory powers or otherwise, will meet the definition of **"directed surveillance"** if it is:

1. covert;
2. likely to reveal private information; and
3. done with some regularity.

The primary consideration is then the privacy setting and whether the person being monitored has a public or private profile. A public profile will allow anyone to see information whereas with a private profile you have to be a friend of the person to see information about them.

4.6 A "one-off" is one on-line visit or a series of three or four visits that are closely connected in purpose, time and stage of the investigation. For example, 3 visits within 2 weeks of each other could be a "one-off" if they relate to the same investigation and are closely related. However, if there is a visit once a week for several weeks that would not be a "one-off" as it would appear to be monitoring the activity of the person.

4.7 It follows that there is no real difference between information from a social media source with public settings and a public website. A "one-off" piece of surveillance therefore would be outside the remit of the RIPA authorisation process.

4.8 Where surveillance is more than a one-off, those involved in considering whether to seek a RIPA authorisation should consider the parallel situation: live, covert observance of a person in public places.

4.9 If there are repeated observances, constituting more than a one-off, then the investigator should consider the real life, parallel situation and relate the use of internet to following a person, covertly, but in public. If an authorisation would be required in the real world, one would also be required in the virtual world.

4.10 Continued covert visits are likely to require RIPA authorisation.

4.11 Further considerations for all will then include the reason for the surveillance and collateral information that may reasonably be suspected of being detected, as a precursor to a procedural application. Generally, the more necessary and proportionate the surveillance, the more likely that a formal application will be required.

4.12 False identities are not unlawful, but real identities of others should not be adopted. However, where there is need to penetrate someone's privacy settings,

by be-friending them by using a false identity or pseudonym, this must be discussed with your manager and a RIPA authorisation will always be required. This can be equated to using a disguise to obtain information about a person, which is directed surveillance and would require RIPA authorisation.

5 Covert Human Intelligence Sources (CHIS)

5.1 Where there is need to apply on-line to join a platform this may require authorisation for use of a CHIS. This will be dependent on the existence of a "relationship."

5.2 If the application to join a site is a formality and there is no interaction with a suspect or their group, this will require a directed surveillance authorisation only.

5.3 The potential for a "relationship" to have been established or maintained must be considered formally with a line manager in such cases, obtaining advice from the Solicitor to the Council as necessary.

5.4 Consideration must be given to the potential for the activity to constitute entrapment.

5.5 These rules apply to the use of any officer or agent of the council.

6 WHAT ISN'T PERMITTED UNDER THIS POLICY

6.1 When it is discovered that an individual under investigation has set their social media account to private, officers should not attempt to circumvent those settings. Such attempts would include, but are not limited to;

- sending "friend" or "follow" requests to the individual,
- setting up or using bogus social media profiles in an attempt to gain access to the individual's private profile,
- contacting the individual through any form of instant messaging or chat function requesting access or information,
- 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, or
- any other method which relies on the use of subterfuge or deception.

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.

6.2 Regardless of whether the social media profile belonging to a suspected offender is set to public or private, it should only ever be used for the purposes of evidence gathering. Interaction or conversation of any kind should be avoided, and at no stage should an officer seek to make contact with the individual through the medium of social media. Any contact that is made may lead to accusations of harassment or, where a level of deception is employed by the officer, entrapment, either of which would be detrimental and potentially fatal to any future prosecution that may be considered.

6.3 If an officer needs to carry out any of the above, then this must be discussed with their manager and if necessary be approved by the Corporate Services team and the Solicitor to the Council before any RIPA application is authorised.

7 CAPTURING EVIDENCE

7.1 Once content available from an individual's social media profile has been identified as being relevant to the investigation being undertaken, it needs to be recorded and captured for the purposes of producing as evidence at any potential prosecution. Depending on the nature of the evidence, there are a number of ways in which this may be done.

7.2 Where evidence takes the form of a readable or otherwise 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, onto a hard drive or some other form of storage device, and subsequently printed to a hard copy. The hard copy evidence should then be exhibited in a suitably prepared witness statement in the normal way and retained in line with retention periods.

7.3 Where evidence takes the form of 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 a CD or DVD. Those CD's and/or DVD's should then be exhibited in a suitably prepared witness statement in the normal way. Any difficulties in downloading this kind of evidence should be brought to the attention of the officer's line manager / ICT department who should be able to assist in capturing it.

7.4 When capturing evidence from an individual's public social media profile, steps should be taken to ensure that all relevant aspects of that evidence are recorded effectively. For example, when taking a screenshot of a person's social media profile, the officer doing so should make sure that the time and date are visible on the screenshot in order to prove when the evidence was captured. Likewise, if the evidence being captured is a specific status update or post published on the person's profile, steps should be taken to make sure that the date and time of that status update or post is visible within the screenshot. Without this information, the effectiveness of the evidence is potentially lost as it may not be admissible in court.

7.5 Due to the nature of social media, there is a significant risk of collateral intrusion into third parties' information. This information may be captured alongside that of the suspected offenders. When capturing evidence from a social media profile, steps should be taken to minimise this collateral intrusion either before capturing the evidence, or subsequently through redaction. This might be particularly prevalent on social media profiles promoting certain events, where users are encouraged to interact with each other by posting messages or on photographs where other users may be making comments.

8 General

8.1 Social media accounts must only be accessed on devices belonging to the Council.

8.2 A log must be kept of the use social media in any investigation detailing the reasons why it was necessary to use it, the results found and any collateral damage to other parties. This must be approved by your

manager if it will be used in evidence. A copy of this log can be found at appendix 1

8.3 Before any investigation is carried out that requires RIPA authorisation you should see if you can gather the necessary evidence in an overt manner from a Dover District Council account.

8.4 All investigations, whether overt or covert, should be carried out by the appropriately trained officer for the department. They will be the individual that will carry out the research and gather the necessary evidence. Appropriately trained officers for departments across the Council are as follows:

Department	**Officer**	**Manager**
Regulatory Services	Environmental Crime Officer	Environmental Crime Team Leader
Regulatory Services	Environmental Crime Team Leader	Environmental Protection Manager
Regulatory Services	Technical Support Officer- Enviro Crime	Environmental Crime Team Leader

9 LEGISLATIVE OVERVIEW – LINKS

9.1 The following are relevant to this area and the subject of RIPA authorisations overall:

- Secretary of State and the Office of Surveillance Commissioners Guidance

https://osc.independent.gov.uk/

- Regulation of Investigatory Powers Act 2000

http://www.legislation.gov.uk/ukpga/2000/23/contents

- The Home Office Guidance to Local Authorities on the Protection of Freedoms Act 2012 - Changes to Provisions under RIPA

https://www.gov.uk/government/publications/changes-to-local-authority-use-of-ripa

- Investigatory Powers Act 2016

http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted

- The CHIS/covert surveillance codes of practice

https://www.gov.uk/government/publications/covert-surveillance-and-covert-human-intelligence-sources-codes-of-practice

- The link to the Council's RIPA Policy

https://intranet.dover.gov.uk/Teams/ChiefExecutive/CorporateServices/RIPA.aspx