Colchester City Council

Use of Social media in Investigations Policy and Procedure

2025/26

A guide to the Council's approach to the use of social media in relation to Regulation of Investigatory Powers Act 2000 investigations.

www.colchester.gov.uk

December 2025

USE OF SOCIAL MEDIA IN INVESTIGATIONS

POLICY AND PROCEDURES

CONTENTS

1.0 INTRODUCTION & BACKGROUND

1.1 Social media has become a significant part of many people's lives. By its very nature, Social media accumulates a sizable amount of information about a person's life, from daily routines to specific events. 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. All of 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. The use of information gathered from the various different forms of Social media available can go some way to proving or disproving such things as whether a statement made by a defendant, or an allegation made by a complainant, is truthful or not. However, there is a danger that the use of Social media can be abused, which would have an adverse effect, damaging potential prosecutions and even leave the Council open to complaints 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 It 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 an accused's human rights, nor to require authorisation under RIPA, whilst ensuring that evidence gathered from Social media is captured and presented to court in the correct manner.

1.6 Officers who are involved in investigations, into both individuals and business 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.

2.0 REGULATION OF INVESTIGATORY POWERS ACT 2000 (RIPA)

2.1 With the increasing use of smartphones and personal 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 research into the sites of suspects could fall within the remit of RIPA and therefore require authorisation prior to it being undertaken. Officers should therefore seek advice from Legal Services prior to undertaking any investigation using Social media sites.

2.2 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 officers involved in investigative practices against individuals, regularly review their conduct with respect to investigatory actions. Any investigation is capable of evolving from being one that does not require RIPA authorisation, to one that does, at any point.

2.3 Accordingly, this Policy should be read in conjunction with the Council's current Code of Practice on Covert Surveillance, as well as the statutory codes of practice issued by the Secretary of State and the Office of Surveillance Commissioners' Guidance.

2.4 Instances of repeated and/or regular monitoring of Social media accounts, as opposed to one-off viewing, may require RIPA authorisation. Advice should be sought from Legal Services where it is envisaged that this level of monitoring will be required in relation to a particular investigation. See paragraph 6.2 below.

3.0 WHAT IS MEANT BY 'SOCIAL MEDIA' FOR THE PURPOSES OF THIS POLICY

3.1 Social media, sometimes also referred to as a Social Network, can take many forms. This makes defining Social media, for the purposes of this policy, difficult, however there are some facets which will be common to all forms of Social media.

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. Beyond this, Social media can be very diverse, but will often have some, or all, of the following characteristics;

- The ability to show a list of other users with whom they share a connection; often termed "friends" or "followers",
- The ability to view and browse their list of connections and those made by others within the system
- Hosting capabilities allowing users to post audio, photographs and/or video content that is viewable by others

Social media can include community-based web sites, online discussions forums, chatrooms and other social spaces online as well.

3.3 Current examples of the most popular forms of social media, and therefore the most likely to be of use when conducting investigations into alleged offences, include:

Facebook	Twitter or X	Instagram
LinkedIn	Pintrest	Tumblr
Reddit	Flickr	Google+

3.4 The number and type of Social media available to the public is fluid. In a given year, many new sites can open whilst some of the more established names can wain in popularity. This Policy will concentrate on Social media generally and will not make reference to specific sites or services.

4.0 PRIVACY SETTINGS

4.1 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 otherwise indifferent about who is able to view their information, others prefer to maintain a level of privacy.

4.2 Depending on their intentions, many users will purposely use Social media with no privacy setting applied whatsoever. This could be due to the fact that 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 Social media profile at all times; others may do so for reasons of self-promotion or even vanity. The information publicly available is known as an individual's public profile.

4.3 Those individuals with public profiles who operate on Social media without any, or only limited, forms of privacy settings being activated do so at their own risk. Often, Social media sites will advise its users through its terms and conditions of the implications of not activating privacy controls, namely that all content they publish or share will be viewable by everyone, including sometimes people who, themselves, do not have an account with that provider.

4.4 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 the individual publishing it is allowing everyone to access and use that information, and to associate it with them.

4.5 The opposite of a public profile is a private profile. Some users of Social media will not wish for their content, information or interactions to be viewable to anyone outside of a very small number of people, if any. In these instances, users will normally set a level of privacy on their Social media profiles that reflects what they are comfortable with being made available, meaning that, for example, only friends, family and other pre-approved users are able to view their content or contact them through that site.

4.6 By setting their profile to private, 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 Human Rights Act. 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.

5.0 WHAT IS PERMITTED UNDER THIS POLICY

5.1 Whether or not Social media can be used in the course of investigating an offence, or potential offence, will depend on a number of things, not least of which is whether the suspect has a Social media presence at all. Investigating offences will always be a multi-layered exercise utilising all manner of techniques, and it is important not to place too high an emphasis on the use of Social media in place of more traditional investigative approaches.

5.2 Further to this, a lack of information on an individual's Social media profile should not be taken as evidence that something is or is not true. For example, a lack of evidence corroborating an individual's assertions that they were at a particular location on a specific day does not prove that they are being misleading and it is important to consider it only as part of a well-rounded investigation.

5.3 For those individuals who do have a presence on Social media, a lot of what is permitted under this policy for use in investigations will depend on whether they have a public or private profile. As outlined in 4.4 above, where a person publishes content on a public profile, they allow everyone, including those not on that particular Social media platform, to access and use that information whilst also allowing it to be associated with them.

5.4 In practice, this means that things such as photographs, video content or any other relevant information posted by individuals and businesses to a public profile on any given Social media platform can be viewed, recorded and ultimately used as evidence against them should the matter end in legal proceedings, subject to the usual rules of evidence.

5.5 When considering what is available on an individual's public Social media profile, those investigating an offence, or potential offence, should always keep in mind what relevance it has to that investigation. Only information that is relevant to the investigation at hand, and goes some way toward proving the offence, should be gathered. If there is any doubt as to whether something is relevant, then advice should be sought from Legal Services.

6.0 WHAT IS NOT 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 under any circumstances. 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 A distinction is made between one-off and repeated visits to an individual's Social media profile. As outlined at paragraph 2 above, a RIPA authorisation must be sought in order to carry out directed surveillance against an individual. Whilst one-off visits, or otherwise infrequent visits spread out 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, for example, be routinely monitored on a daily or weekly basis in search of updates, as this will require RIPA authorisation, the absence of which is an offence. For further guidance on this point, officers should contact Legal Services.

6.3 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 at all costs, and at no stage should a Council 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.

7.0 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 to a suitably prepared witness statement in the normal way.

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 to 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 Council's IT Team who will 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 Council 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 suspected offender'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 damage in the form of other, innocent parties' information being inadvertently captured alongside that of the suspected offenders. When capturing evidence from a Social media profile, steps should be taken to minimise this collateral damage 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.

8.0 OTHER INFORMATION TECHNOLOGY TOOLS AVAILABLE FOR INVESTIGATIVE PURPOSES

8.1 Whilst Social media can be a useful and fruitful means of investigating offences and potential offences, it is by no means the only tool available within the realm of Information Technology. A vast array of other, mostly web-based tools are also at the disposal of those conducting investigations. For example, where there is a website advertising the services of a local business, and there is evidence that this business is engaging in illegal activity, there are IT tools available that can track who is responsible for setting up that website, and so can be a good starting point when trying to link potential offenders to the offending business.

8.2 For assistance in identifying which tools may be appropriate, and how best to utilise them, advice should be sought from the Legal Services and or the Council's IT team.

9.0 RETENTION AND DESTRUCTION OF INFORMATION

9.1 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 **not** be destroyed, but retained in accordance with the requirements of the Data Protection Act 2018 , the Freedom of Information

Act 2000, and any other legal requirements, including those of confidentiality, and the Council's policies and procedures regarding document retention. Advice should be sought from the Data Protection Officer or the Monitoring Officer.

9.2 Personal data gathered by the Council is subject to the Data Protection Act 2018. When considering whether to retain the data, the Council should:

- review the length of time it keeps personal data;
- consider the purpose or purposes it holds the information for in deciding whether (and for how long) to retain it;
- ensure that there is a lawful basis for processing the personal data
- securely delete information that is no longer needed for this purpose or these purposes; and
- update, archive or securely delete information if it goes out of date
- ensure that whilst data is held it is kept secure at all times

9.3 Due to the nature of Social media, it is important to remember that when information produced as a hard copy is destroyed in line with this paragraph, that all digital copies of that evidence is likewise destroyed.

10.0 REVIEW

10.1 This Policy will be reviewed annually in line with the Council's Code of Practice on Covert Surveillance to ensure that both documents remain current and compliant with relevant legal requirements and best practice guidance.