Northumberland
County Council

Corporate Fraud Team

Internet Investigations Policy

(The use of Social Media and similar related sites)

Policy Title: Internet Investigations Policy
Version: 1.0
Policy Author: Barry Haigh
(Created Feb 2018 Review date Feb 19)

1 Introduction

1.1 The advent of social media sites has created the ability for individuals, businesses and organisations to easily communicate between each other, serving as a useful tool to keep in touch and interact on what can be a real time basis.

1.2 People or groups can instantaneously share information, coordinate events and provide updates that are of interest to their friends, family, or customer base.

1.3 Social media sites can also serve as a platform for individuals or groups to express their opinions and social, political and religious beliefs to give just a few common examples.

1.4 It is also possible to share photographs or videos with others and indeed where privacy settings allow, to share the posts of other people not necessarily connected with the original person.

1.5 Online research and investigation has therefore become an extremely useful tool for investigators to prevent, detect and investigate potential criminal activity.

1.6 It also presents new challenges as the use of such methods can still interfere with a person's right to respect for their private and family life which is enshrined in Article 8 of the Human Rights Act and the European Convention on Human Rights.

1.7 Public Authorities must ensure that any interference with this right is:

- Necessary for a specific and legitimate objective – such as preventing or detecting crime;
- Proportionate to the objective in question;
- In accordance with the law.

1.8 Whenever you are using the internet to gather intelligence or evidence you must consider whether you are likely to interfere with a person's private and family life and, if so, whether you should seek authorisation under the Regulation of Investigatory Powers Act for your conduct.

1.9 It is also essential to consider the effect of any collateral intrusion on the private and family life of other people not directly connected with the subject of the research or investigation.

1.10 Case by case judgement is vital when researching or investigating online.

1.11 This policy therefore sets out a clear framework for the use of social media and other similar sites during the course of investigations.

2 Legal Framework

2.1 Online research and investigation techniques may be affected by any or all of the following legislation

- Human Rights Act 1998 (HRA)
- European Convention on Human Rights (ECHR)
- Regulation of Investigatory Powers Act 2000 (RIPA)
- Data Protection Act 1998 (DPA)

2.2 Human Rights Act / European Convention on Human Rights

2.3 The right most likely to be engaged by staff undertaking online research and investigation is Article 8 which states:

8.1 - Everyone has the right to respect for his private and family life, his home and his correspondence.

8.2 - There shall be no interference by a public authority with the exercise of this right except such as is in accordance with the law and is necessary in a democratic society in the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals or for the protection of the rights and freedoms of others.

2.4 Ensuring that RIPA authorisations are sought, where necessary, and that the material obtained is retained and processed in accordance with the provisions of the Data Protection Act should provide the lawful authority required by Article 8.2 for any perceived interference with Article 8.1.

2.5 Regulation of Investigatory Powers Act 2000 (RIPA)

2.6 Under 26(2) of RIPA, surveillance is “directed” if it is covert but is not intrusive and is undertaken:

- For the purposes of a specific investigation or a specific operation;
- Is likely to result in the obtaining of private information about a person;

  and

- Is otherwise than by way of an immediate response to events or circumstances the nature of which is such that it would not be reasonably practicable for an authorisation under RIPA to be sought

for the carrying out of the surveillance.

2.7 Whether or not there is a likelihood of obtaining private information will be a determining factor when considering if an authorisation as directed surveillance will be appropriate.

2.8 Private information is information relating to a person's private or family life. It can include any aspect of a person's relationships with others, including professional or business relationships.

2.9 A person may have a reduced expectation of privacy when in a public place but covert surveillance of their activities in public may still result in the obtaining of private information.

2.10 This principle applies equally to the online world, including social media sites, where access controls set by the owner of the information may be a determining factor in considering whether information posted on the internet is publicly available or whether, by applying the access controls, the owner has removed the information from a wholly public space to a more private space where the information could be considered as private.

2.11 Unrestricted open source information is unlikely to fall within the definition of private information.

2.12 Data Protection Act 1998 (DPA)

2.13 The DPA guiding principles are that personal data must be processed fairly and lawfully, must not be processed in a manner that is not compatible with the purpose for which it was obtained, must be relevant and adequate but not excessive and must not be kept longer than is required.

2.14 Much of the information obtained by online research and investigation will meet the definition of personal data. Case law has established that the processing of personal data is capable of interfering with a person's Article 8 right to respect for their private and family life, irrespective of whether the information was obtained under a RIPA authorisation or not.

3 Open Source Information

3.1 Most of the information available on the internet is available to any person with internet access. Such information is widely known as open source information.

3.2 Viewing open source information does not amount to obtaining private information because that information is publicly available. This is therefore unlikely to require authorisation under RIPA whether it is done on a one off basis or by repeated viewing.

3.3 Recording, storing and using open source information in order to build up a profile of a person or group of people must be both necessary and proportionate and, to ensure that any resultant interference with a person's Article 8 right to respect for their private and family life is lawful, it must be retained and processed in accordance with the principles of the DPA.

3.4 In relation to open source material the following definitions are provided to assist those involved in online research and investigation;

- Open source research – the collection, evaluation and analysis of materials from sources available to the public, whether on payment or otherwise, to use as intelligence or evidence in investigations.

- Open source information – publicly available information, i.e. any member of the public could lawfully obtain the information by request or observation.

3.5 Whilst it is unlikely that the viewing of such information on a repeated basis will amount to surveillance, each site should be assessed on a case by case basis.

3.6 It may not, for example, be proportionate to view a Facebook profile on numerous repeated occasions within a short space of time and, for this reason, it is recommended that such viewings be limited to a maximum of 3 within any 28 day period.

3.7 Under these circumstances a log should be maintained within the investigation file detailing the date and time of each visit and a brief note of the information gained.

4 Restricted Access Information

4.1 Access to some of the information on the internet is restricted by the owner, for example a common form of restriction is in social networks where a profile owner may use the privacy settings to restrict the access to online "friends".

4.2 Privacy settings are covered fully in Section Five below.

4.3 Viewing restricted access information covertly will generally constitute covert surveillance and, as the information is not publicly available, it is likely that private information will be obtained.

4.4 Under these circumstances an appropriate authorisation under RIPA should be sought.

4.5 It should be noted that the use of a false persona in an attempt to bypass privacy controls and gain access to restricted information, i.e. by sending a

false “friend” request, is expressly forbidden.

4.6 Using the Facebook example the profile maintained by the Corporate Fraud Team should normally be used for all research and investigation purposes although it is permissible for individual members of staff to use their own personal profiles although this should not be undertaken from home unless the computer is connected to the council network.

4.7 In all cases it must be remembered that any online research or investigation leaves a trace or “footprint” which can be tracked back to the council.

4.8 Recording, storing and using restricted access information must be dealt with in accordance with the principles outlined above in section 3.3.

5 Privacy Settings

5.1 Most Social Media Sites will have a variety of privacy settings that users can apply to restrict information and protect their accounts from others accessing such information.

5.2 Using Facebook as an example, depending on what privacy setting a user chooses, different people can access the account and see some or all of the content.

5.3 Public Setting

5.4 All Facebook users can see the account and all of its content, including the user’s “friends”, their timeline and photographs. Non-Facebook users can see photographs and posts published on the account, but not who has “liked” a post or the marital status and geographic location of the user.

5.5 “Friends” Setting

5.6 Only those who the user has accepted as Facebook “friends” are able to see the entire content of the user’s page.

5.7 Custom Setting

5.8 The user can create lists of specific contacts and Facebook users and designate them as the audience for, for block them from view of, any posts.

5.9 Of the three options outlined above the only available resource normally available to investigators is the public profile although as indicated in Section Six below there may be limited occasions where the “friend” profile may become available.

6 Utilisation of Social Media Information

6.1 Surveillance using the Investigator's private account

6.2 If an Investigator views a user's profile with whom they are not "friends" and where the content is not protected by any privacy settings, then information on this profile can be treated as being in the public domain. Visiting/viewing this profile will accordingly be overt and no authorisation under RIPA will be required.

6.3 If the Investigator frequently or regularly visits/views the same individual's profile this must be considered as targeted surveillance. However if the user posts publically, they can have no expectation of privacy and will give everybody the right to view their posts at any time and as many times as that person wishes. No authorisation under RIPA is therefore required although the provisions of sections 3.6 and 3.7 above will apply.

6.4 The Investigator may not under any circumstances send a "friend" request or attempt to contact the user unless that user is already a "friend" in a personal capacity.

6.5 Surveillance using the Corporate Fraud Team account

6.6 Where the Investigator visits/views a user's account which is not protected by any privacy settings then the provisions of sections 6.2 and 6.3 above will apply.

6.7 To investigate a user whose account is protected by privacy settings, with the specific approval of the Corporate Fraud Manager it is permissible for a "friend" request to be sent to the user.

6.8 It is also permissible for the Investigator to communicate with the user via the account provided specific approval has been granted by the Corporate Fraud Manager.

6.9 In all cases the approval in relation to section 6.7 and/or 6.8 is to be clearly noted in the investigation file.

6.10 As it will be obvious that the "friend" request or communication has originated from the Corporate Fraud Team then such action is not classed as covert and accordingly no authorisation under RIPA will be required.

7 Conclusion

7.1 The use of social media as an investigation tool is constantly evolving and it is not therefore intended that this policy will cover all eventualities.

7.2 Whilst it is unlikely that any form of RIPA authorisation will be necessary this aspect must be considered by Investigators and, as outlined above in

Section 1.7 great care must be taken to ensure that there is no interference with a person's right to respect for their private and family life.

7.3 Where there is any doubt regarding the use of this policy advice should be sought from the Corporate Fraud Manager;

Barry Haigh, Corporate Fraud Manager
Telephone: 01670 624273
Email: barry.haigh@northumberland.gov.uk

Appendix One

Guidance issued by the Chief Surveillance Commissioner

The following has been extracted from the Office of the Surveillance Commissioner Procedures and Guidance Document (December 2014) in relation to the covert surveillance of Social Networking Sites (SNS).

288 The fact that digital investigation is routine or easy to conduct does not reduce the need for authorisation. Care must be taken to understand how the SNS being used works. Authorising Officers 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.

288.1 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). Where privacy settings are available but not applied the data may be considered open source and an authorisation is not usually required. Repeat viewing of “open source” sites may constitute directed surveillance on a case by case basis and this should be borne in mind.

288.2 Providing there is no warrant authorising interception in accordance with section 48(4) of the 2000 Act, if it is necessary and proportionate for a public authority to breach covertly access controls, the minimum requirement is an authorisation for directed surveillance. An authorisation for the use and conduct of a CHIS is necessary if a relationship is established or maintained by a member of a public authority or by a person acting on its behalf (i.e. the activity is more than mere reading of the site’s content).

288.3 It is not unlawful for a member of a public authority to set up a false identity but it is inadvisable for a member of a public authority to do so for a covert purpose without authorisation. Using photographs of other persons without their permission to support the false identity infringes other laws.

288.4 A member of a public authority should not adopt the identity of a person known, or likely to be known, to the subject of interest or users of the site without authorisation, and without the consent of the person whose identity is used, and without considering the protection of that person. The consent must be explicit (i.e. the person from whom consent is

sought must agree (preferably in writing) what is and is not to be done).