Appendix 1

Gloucester City Council
Social Media Policy for the purposes of the Regulation of Investigatory Powers Act 2000' RIPA'

Gloucester City Council recognises the benefits and opportunities that the internet and multi-media provide to access and share information using a wide range of on line facilities. This is referred to Social Networking Sites – 'SNS'.

There are however some considerations and standards to apply when using such sites and this policy establishes the Council's position regarding the use of the internet, mobile web browsing and specifically social media websites when undertaking investigations under and in accordance with RIPA.

The Council's ICT Security Policy provide the basis for this policy and associated guidance. This policy should be read in conjunction with the supporting RIPA Policy and any guidance issued by the OSC – Office of the Surveillance Commissioners.

This policy covers external investigations, which could also apply to internal staff that may be subject to an investigation. Advice should be taken from HR should an investigation involve a member of staff.

Contents.

Scope.

1. This policy covers the use of social media, including social networking websites such as Twitter, Facebook, LinkedIn, and YouTube, content communities and blogs.

2. The policy and guidance aim to ensure that the council and its employees when undertaking investigations are protected and that a lawful and fair process is followed.

3. This policy closely relates to other council documents but in particular ICT Security policy.

4. The other legislation that may also be impacted by an investigation being carried out is as follows: Human Rights Act 1998, Freedom of Information Act 2000 and the Data Protection Act 1998

The use of conducting an investigation under the Social Media Policy.

5. The implications of enforcement monitoring through the use of social and human rights implications is a difficult area for law enforcement with complex privacy considerations:

5.1 The two main issues are:

(i) What expectation of privacy a user may reasonably have when posting on the Internet; and
(ii) How covert or overt the officer looking at information on the internet is being.
(iii) Whether or not a RIPA or CHIS authorisation should be obtained.

<u>Investigatory 'Tools'</u>

6. There are three main investigatory tools under RIPA that Trading Standard's Officers 'TSO' may consider using in an investigation involving SNS. They are:

6.1 The use of 'Directed Surveillance, which is essentially covert surveillance carried out in places other than residential premises or private vehicles which is relevant where an investigatory technique might infringe Article 8 rights (e.g. where personal data or sensitive is likely to be accessed or acquired and there is an expectation of privacy) and which is subject to a 'crime threshold' when investigating criminal offences.

6.2 The use of Covert Human Intelligence Source (CHIS) which includes undercover officers (most significantly included covert profiles), informants and persons making test purchases; and

6.3 Powers to acquire or obtain 'communications data'.

6.4 The Council is seeking to focus on 3 broad categories so as to give an indication of what is and what is not acceptable for us to do. Prior to starting a browsing session an officer should consider what he/she is seeking to achieve and is likely to be doing and be aware of when their actions might cross the boundary from one "level" to another.

Three Broad Categories

7. **Category 1** – Viewing publically available postings or websites where **the person viewing does not have to register a profile, answer a question, or enter any significant correspondence in order to view.** E.g. a typical trader's website.

- There must be a low expectation of privacy and **no RIPA authorisation would normally** be required to view or record these pages.

- However, **repeated visits** over time to the extent that you might be perceived as **monitoring** a website, may require authorisation. Private information can remain private information even when posted on such a website and the European Convention on Human Rights has construed that the way a business is run can be private information. If you intend to monitor in this way therefore you may acquire private information and it is recommended that it is done in a **systematic** way with results recorded. Particularly note whether or not you happen to access private information. The fact that on previous visits a lack of private information is found could be good evidence that any subsequent acquisition was incidental and a RIPA authorisation is not required.

- There is unlikely to be **unfairness** (S78 PACE Act) in presenting the pages viewed as evidence. Pay attention to the requirements in Appendix B of the ACPO Good Practice Guide for Digital Evidence (in Chapter 2 of the D&S enforcement manual). If a test purchase is required, we may use a fictitious name and address without triggering the need for a CHIS (or Directed Surveillance) authorisation, provided no "relationship" is formed.

- As above, the **use of a fictitious identity or "covert" account** is not necessarily the trigger for a need for a RIPA authorisation, be it Directed Surveillance, or the in the case of a test purchase, CHIS. More relevant is the likelihood of acquisition of private information, or how far a "relationship" is formed.

8. **Category 2** – Viewing postings on social networks **where the viewer has had to register a profile but there is not otherwise a restriction on access**. This would include Facebook where there is no need to be accepted as a "friend" to view. E.g.: Trader has a "shop window" on Facebook advertising a business and products.

- There are differences between this and Category 1. The person who posts information or runs such a website may reasonably expect viewers to work within the terms and conditions of the website.

- Viewing should therefore normally be conducted in an overt manner i.e. via an account profile which uses your correct name, and email address (which should be a devon.gov.uk etc. address) or an appropriate Officer set and sanctioned profile. If this is done I can see no objection to a recording of the visit being made and presented evidentially.

- If the posting or website contains no private information a viewing would not engage privacy issues and therefore a RIPA authorisation is not needed. However it is possible that a mixture of private and business material is displayed, and the ECHR has construed the way a business is run as being private information. The conditions regarding **repeat visits** in Level 1 are therefore relevant.

- A "Covert" account at this level should only be used in the context of a RIPA authorisation.

9. **Category 3– Viewing postings on social networks which require a "friend" or similar status to view.**

    - These are **highly** likely to involve viewing private information.

    - Repeated viewings will constitute Surveillance and require a RIPA authorisation. This may apply whether or not a "covert" or "overt" account is used, though this is probably best obtained via a CHIS authorisation with the use of a covert profile and appropriate risk assessments.

    - An "Overt" account which gains "friend" or similar status may **still require a RIPA authorisation.** It may be that such a status may be given by a default on the part of the person posting or website owner. The TSO should be especially sure that their access is being granted as a representative of the Trading Standards Service. For example, on Facebook it is stated that only people who know the person who maintains a profile should send a "friend" request to that profile. A person accepting that friend request may believe the person requesting is an acquaintance that they simply do not recall or know by another name. They still have a justifiable expectation of privacy. While requesting access may not comply with a strict interpretation of Facebook terms and conditions, a clearly identifiable **Trading Standards Officer's Service Sanctioned profile** is a way to deal with that expectation of privacy, rather than a more neutral officer based profile.

    - An appropriate Officer set and sanctioned profile is currently being set up to be run in order to obtain intelligence and provide advice.

    - A "Covert" account at this level should only be used in the context of a RIPA authorisation.

Covert Facebook Accounts:

10. The use of covert Facebook accounts to access postings need to be covered by a RIPA authorisation. Currently there does not seem to be a mechanism for Trading Standards to operate these on Facebook within the company's terms and conditions. Any evidence obtained via them can run a risk of being considered "unfair". It is quite likely that the profiles used will become "blown" at some stage and users need to monitor them to ensure this is identified early. Considerable officer time is required to maintain a covert identity.

11. Obtaining a RIPA authorisation will also present an officer with a defence should there be an allegation that they have breached the Computer Misuse Act 1990 – it is an offence to deliberately access unauthorised material.

Covert surveillance of Social Networking Sites (SNS)

12. 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.

13. 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.**

14. 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).

15. **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.

16. 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).

Recording Information

17. All information should be recorded on the appropriate form(s) should an authorisation be required.

Training

18. Training should be made available to Officers undertaking any covert or directed surveillance when undertaking investigations.

Useful Contacts

19. Helpline@saferinternet.org.uk

Related Documents

20. Documents that should be referred to are:
    - RIPA Policy
    - Office of Surveillance Commissioners
    - Code of Conduct
    - ICT Security Policy
    - ICT User Guide