

ANNEX B to RIPA Policy

Guidance on the use of Social Networking Sites for investigations

It is recognised that the use of the internet and, in particular, social networking sites, can provide useful information for South Hams District Council and West Devon Borough Council staff carrying out investigations. These investigations may relate to the various enforcement roles within the council – for example Fraud, Planning Enforcement, Licensing or Environmental Health, but will equally apply to some non-enforcement teams, such as Debt Collection or Housing. The use of the internet and social networking sites may fall within the definition of covert directed surveillance. This is likely to result in the breaching of an individual's Article 8 rights under the Human Rights Act (the right to privacy).

Social Networking Sites

There is a fine line between general observation, systematic observation and research and it is unwise to rely on a perception of a person's reasonable expectations or their ability to control their personal data.' The Councils' policy in relation to the use of social media for the gathering of evidence to assist in its enforcement activities is set out below:

- Officers of South Hams and West Devon must not 'friend' individuals on social networks as part of undertaking their roles and should not use their own private social networking accounts to view the social networking accounts of other individuals as part of their professional role
- officers viewing an individual's profile on a social networking site should do so only once in order to obtain evidence to support or refute their investigation
- further viewing of open profiles on social networking sites to gather evidence or to monitor an individual's status, must only take place once RIPA authorisation has been granted and approved by a Magistrate
- officers should be aware that it may not be possible to verify the accuracy of information on social networking sites and, if such information is to be used as evidence, steps must be taken to ensure its validity.

The **purpose** of this guidance note is to provide clarity on the Councils' position:

1. It is not possible to provide a definitive list of social networking sites, so this should be taken to mean any site which involves individuals creating a profile which contains personal information and is viewable by others, whether accepted as 'friends' or otherwise. This might include sites such as 'Facebook' and 'LinkedIn'
2. As the definition of 'private information' under RIPA includes:

'any information relating to a person's private or family life and should be taken generally to include any aspect of a person's private or personal relationship with others, including family and professional or business relationships'

Sites used to advertise goods and services should be included within the definition. Although there is likely to be a reduced expectation of privacy with this type of site, there is still the possibility of obtaining private information which may be subsequently used in any enforcement proceedings.

3. If an allegation is received or, as part of an investigation into an individual, it is necessary to view their social networking site, officers may access the main page of the individual's profile once in order to take an initial view as to whether there is any substance to the allegation or matter being investigated.

4. The initial viewing must be reasonable – for example, it would not be reasonable to spend any significant amount of time searching through various pages of the individual's profile or to print out several pages just in case they may reveal something useful.

5. In some cases where, for example, a link to a site is provided by a complainant, it may be relevant for the receiving officer to view the link before passing it onto the investigating officer to also view. This would count as one viewing. However, it would not be reasonable for each officer in a team to view the site in turn so that they may each gather some information.

6. Each single viewing of an individual's social networking site must be recorded on the log maintained by Legal Services (RIPA Co-ordinating Officer). This is to enable the reporting of the number of viewings to the Overview & Scrutiny Committee of each Council.

7. If it is considered that there is a need to monitor an individual's social networking site, authorisation must be obtained from an Authorising Officer.

8. If the offence being investigated falls under RIPA, a formal RIPA application must be completed, authorised by one of the Councils' Authorising Officers and then approved by a Magistrate.

9. If the offence being investigated falls outside of RIPA (for example if the offence does not carry a custodial sentence of at least 6 months imprisonment or is not a core function of the council) a non-RIPA form must be completed. General guidance on RIPA and appropriate forms can be found on the Councils' Intranet and in the main RIPA Policy document.