Do you use the internet and social media to obtain information about others?

If you use the internet and social media to obtain information about others, make sure you are aware that you need to comply with legal rules and follow council procedures.

With advances in technology making it easier, quicker and increasingly popular for individuals to share personal information on-line, the opportunities to use that information for research, investigative or other official purposes are expanding too.

However, it is important to appreciate that the considerations of privacy which arise in the physical world also arise in the on-line world. In other words, there are rules and there are limits.

Just because many social media sites and other information on the internet is freely accessible does not mean that officers can openly access such information without careful regard to the constraints and requirements of the law.

How do I know if I need to comply with the law?

Repeated or systematic viewing, collecting or recording of private information from 'open' on-line sources (such as Facebook, Twitter, Snapchat and LinkedIn), including information relating to the interests, activities and movements of individuals, and others associated with them, could be regarded as a form of covert surveillance.

In addition, it is likely that individuals will have a reasonable expectation that their information is not used for surveillance purposes by public authorities and therefore may complain that their privacy and human rights have been infringed.

Initial research of social media to establish or check some basic facts is unlikely to be a problem but repeated visits to build a profile of an individual's lifestyle etc. is likely to assume legal significance depending on the particular facts and circumstances. This is the case even if the information is publicly accessible because the individual has not applied any privacy settings.

REMEMBER: There are legal rules governing the use of covert surveillance by local authorities. It has to be appropriate and proportionate, authorised in writing by a senior officer first and, in some circumstances, approved by a magistrate too (see here for a short guide on the law: RIPA Short Guide.7July2017.pdf).

The council is regularly inspected by an external organisation to check that these rules are followed. The concern expressed by this Government watchdog is that whilst regulatory officers working in council trading standards and benefit fraud teams will be familiar with the rules and procedures, others such as social workers who may only occasionally and acting on their own initiative use social media sites to mine for information for safeguarding and other legitimate purposes may not be.

It is also really important to appreciate that if you obtain, use or even merely store information about individuals you have to comply with data protection rules. And, as recently published on the intranet and on Yammer, with less than a year before the council will have to comply with new data protection laws, the information the council collects about individuals, how and why will have to comply with stricter transparency and accountability rules.

So what do you need to do?

It would be really helpful if you could discuss and document in your teams when you use the internet and social media sites for investigative, research or other council business. **Please give as many specific examples as you can.** We will then use the information gathered to provide further guidance.