

## Web 2.0 and Social Networking Sites

### Concerns and Guidelines

**Web 2.0 is commonly accepted “shorthand” to describe the metamorphosis of the Internet from a one directional, publisher to user, medium into a more completely interactive two-way medium - with increasing emphasis on user generated and contributed content. Whilst social networking in the business context can be beneficial, as always, the downside should not be overlooked.**

#### Background

Those completely unfamiliar with this territory may wish to look at the Information Commissioner's website ([www.ico.gov.uk](http://www.ico.gov.uk)) (click on the character on the left hand side of the home page) for the Information Commissioner's advice guidelines which, although aimed at teenagers, give a useful introduction to the world of social networking sites - and their implications. The need for advice was borne out of the startling results of a survey commissioned by the ICO<sup>1</sup> which, amongst other things, indicated that:

- Nearly 1/3 of those surveyed never read privacy policies on websites they sign up to; nonetheless 95% would be concerned about the ability of such websites to use their details (which commonly include DOB, e-mail address, mobile phone number etc.) to target advertising at them and most wouldn't want a College, University or potential employer to conduct an internet search on them unless they could first remove content from social networking sites.
- 66% have accepted someone on a social networking site, who they didn't know personally, as a friend - a finding rather corroborated by another study by leading Internet security firm Sophos<sup>2</sup> that 41% of Facebook users were prepared to disclose personal information to a complete stranger called “Freddi Staur”<sup>3</sup> (crossword experts will already have worked this one out).

#### Concerns

A whole raft of dangers for **individuals** will be self evident from the above - identity theft, increased spam or other unwanted marketing, threats and risks to privacy and even personal safety - all stemming from careless posting of information which you lose the ability to control once it has left your computer.

Following the guidelines produced by organisations such as ICO and Sophos (in particular the correct use of privacy settings) will reduce these risks.

Placed in the **business** setting the risks and downsides are equally worrying:

- The sheer wastage of working hours through time spent on social networking sites.
- The lack of control exercisable over site content. Regrettably many sites are havens for bullying and harassment - particularly prevalent in the teacher/pupil school environment but just as damaging to the image of an employer whose business or one or more employees is the subject of unjustified criticism, abuse or insult.
- The risk of data leakage (with Data Protection Act and confidentiality implications) and network damage through viruses or hackers as well as heightened risk of cyber crime - bearing in mind that employees may well post employment and other business details on a site (enabling fraudsters to guess network passwords etc.).

#### Action Points

As always, in the workplace, matters are best regulated by a clear policy (part of your overall technology policy, in turn forming part of the employment contract) on the do's and don'ts of using external Web 2.0 services. However, faced with the added work, time and responsibility which this involves, businesses can scarcely be blamed for taking the view that banning workplace access to social networking sites is the more certain alternative - and this is exactly what the firewalls on many school networks do. Clearly however, this is only part of the story as the use of mobile phones or home PCs cannot be controlled in this way.

Until the social networking phenomenon is overtaken by some other advance in technology (as it undoubtedly will be) businesses would do well to tighten up network security and minimise the risk of financial or reputational damage through a combination of appropriate technical measures and rigorously enforced workplace rules on appropriate Web 2.0 usage.

For further information on any aspect of intellectual property please contact Lester Cameron ([LFCameron@paul-williamsons.co.uk](mailto:LFCameron@paul-williamsons.co.uk))

<sup>1</sup> Topline Report - Oct. 2007

<sup>2</sup> [www.sophos.com](http://www.sophos.com)

<sup>3</sup> anag. “ID Fraudster”