Guidelines for Using Social Networking Sites

1. Introduction

Social networking sites such as Facebook, Beebo, YouTube, Twitter etc have become very much part of our everyday life as we use them to keep up with friends, share photographs exchange ideas and so on.

These sites work by sharing information with others: but how much information do you want to share? Would you tell a complete stranger where you were last night, with whom, what you did and to whom? Probably not, but when you use these social networking sites you could be doing just that unless you take some simple precautions.

So stop and think for a moment: when a web or social networking site is asking you to provide personal information…….

- Do you know who has access to the information?
- Do you know how the information will be used?
- Are you happy to share this personal information?

You probably don't know the answer to these questions so let's have a look at what could be going on in the background and how you can protect your privacy and private life.

2. Security

Security is very important and you need to know whether the site is secure or not. Look for a yellow padlock symbol in the bottom right corner of the screen. 

If it is displayed then it is probably safe to enter very personal details like your credit card number and other such personal details. Be wary of organisations that you might think are trustworthy: if there is no padlock symbol displayed it's not secure. But even if the padlock symbol is displayed, be cautious: clever programmers can "edit" web pages and insert spoof symbols.

Check the site's privacy statement to see what you are signing up to. This may seem like a chore, but may save you from lots of trouble later on. You need to know whether the site will protect your details, whether they take ownership of the data you put up to the site and whether they enforce their privacy policy. If in doubt, don't (unless you are prepared to run the risk of your data getting into the wrong hands).

3. Protect your identity!

OK so you put personal information onto a social networking site: who's going to benefit from this? Networking sites make money by selling information to marketing companies who in turn use it to try and sell things to you and you friends. The more users a site can get the higher a price it can charge for its information. It will pay you to check the sites privacy policy to see what they do with your information.

It's therefore very important you protect your identity. Most social networking sites have privacy settings that allow you to determine who can see your user profile and contact information. It's a good idea to set up an e-mail account specifically for use with social networking sites. Keep it completely separate from your normal e-mail account. The name you use should not be your real name, but choose your screen name with care to avoid unnecessary (and potentially unwelcome) attention. Who knows what images names conjure up in some people's minds! Whatever you do don't use your real name, e-mail address or any other information that would enable someone to identify you.

Having chosen a screen name, only share it with those you really trust. Take very great care in responding to requests for information about yourself. Think, just who is the requestor and why is this information being sought? Be especially careful of requests for financial information or exceptionally good financial offers: they are rarely what they seem!

Finally, remember it's not just your identity you are protecting, it's also all your friends', your family, anyone about whom you have published information whose identities you need to protect.

4. Watch out for cookies!

Cookies are files which web sites use to store information about you. Most are fairly harmless, but over a period of time the file will build up a dossier of information about you, your interests and activities. This can be sold on to marketing companies who will use the information to target you with specific advertising. However, they can equally be used by the unscrupulous to set up frauds and other criminal activities. Most internet browsers can be set to tell you when a cookie is installed and Microsoft Internet Explorer will allow you to block cookies. Be aware!

The search engines you use log your IP address (that's the exact computer you are using), the search string, cookies launched, date time and so on. Your search is not anonymous and the data may come back to haunt you in the future.

5. Be careful what you say or show.

Be very careful what you say or show about yourself or anyone else! Don't post details you or anyone else might find embarrassing or you don't want family, lecturers, and potential employers etc to know. Accessing social networking sites from University computers means you are bound by the University's Acceptable Use Policy. So don't:

- Say defamatory things about people or organisations
- Say anything that is racially motivated
- Engage in any commercial activity
- Engage in any criminal activity
- Tell lies
- Post inappropriate pictures or videos

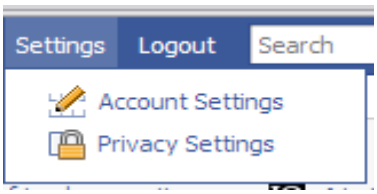
Breach of the policy will render you liable to disciplinary action. Is it really worth the risk?

6. Long live the data

Once you have posted information to a web site, it can be almost impossible to remove it because of file sharing, archiving and other considerations. Even if you unsubscribe from a site, your information may remain visible for a long time.

7. I want to use Facebook – how do it do it safely?

Facebook has a number of options that will restrict who can see what in your account so it is worthwhile spending a few minutes setting the account up. The default setting is to make **all** your information visible by all your friends and networks; potentially several hundred thousand people! Public search listings make limited information about you (your name and profile picture) available to people who are not logged in to Facebook. This information is available to search engines like Google.



When you first register, enter only very basic information about yourself. Then click on the **Privacy** option at the top of the screen and adjust the settings before adding any more information about yourself. If you want to add a picture of your self, use one that is not immediately identifiable as you i.e. out of focus or a caricature. If your picture includes other people, make sure you have their permission before posting it to Facebook.

Set profile privacy settings to:

- "only my friends"
- "Photos tagged of you" and "Videos tagged of you" to "Only My Friends"
- Contact information: consider setting this to "No-one" (the default is "Only My Friends")

'Search' privacy settings:

- 'Who can find me in search' – Default is "all my networks and all of my friends".
- Only choose "Everyone" if you are willing to let **anyone** see you are in Facebook
- Deselect the "Allow my public search listing to be indexed by external search engines"

Facebook 'walkthrough' - adjusting your privacy settings - gives step-by-step guidance on adjusting your privacy settings and explains why you should consider choosing the more private options.

So who's my friend? Once you have nominated someone as a friend, they will be able to see all information, including photographs and videos you have marked as "viewable by friends". Is that what you want? You can make people "limited friends" which gives them access to a cut down version of your profile. This useful for people you might class as "associates", people you are not happy about sharing your full personal information with.

8. Are there any other dangers I should be aware of?

Yes, there's a practice known as "phishing" or "pharming". This is where e-mails are sent randomly and apparently from a well respected organisation to many people. They are aimed at getting you to give away personal information, particularly credit/debit card details which can then be used in all sorts of ways. The messages often contain links which are false and redirect you to a fake website. Phishing is on the increase at the moment and universities seem to be prime targets for these attacks. These are generally well written e-mails, which appear to come from the University helpdesk or central administration and ask for login information. If this is given, the account details are then used to send spam from your account and, of course, your compromised account could be used to access any services you have privileges to, such as your personal details in *my*Course.

This type of emails is not legitimate and should be deleted.

Solent University will NEVER ask staff and students for their passwords by email or phone and you should never offer your password. If you think someone else knows your password, change it immediately! Press the Ctrl, Alt and Delete keys simultaneously and choose the "change password" option.

If you receive a spam e-mail, don't reply to it. You are confirming to the spammers that the account exists and is live. If you are unsure about any e-mails you receive, forward them to lrc.help@solent.ac.uk.

Even if you are fairly certain an e-mail is genuine, do not click the links in the page. Open your internet browser and go directly to the company or organisation and see if you can verify the message by following the links on the genuine webpage. If you can't find the information on the "real" web page, then the original e-mail is almost certainly a phishing attempt.

You can find more information on phishing and internet security in general at www.mcafee.com/us/local_content/white_papers/wp_phishing_pharming.pdf and www.scotiabankpr.com/english/seguridad.asp