

## **Safe use of Social Networks and Social Media for Personal Business**

The rise of social networks such as Facebook, Instagram, and LinkedIn, as well as social media sites such as YouTube, Twitter, and Flickr, has provided Internet users an unprecedented set of tools to create, maintain, and rekindle social and professional relationships. While these social networks and media sites have many useful features, users should be aware of some their downsides, particularly as it relates to use on university computers. These guidelines are intended to address individual use.

As social networks and media sites are designed to make information available, it may be difficult to maintain personal privacy or to restrict information only to certain persons. Some sites may have the ability to harvest your e-mail contacts or personal information and use this information in a way you may not approve.

*Individuals should use caution, particularly when accessing these sites from university computers.*

Below are general principles for individuals to follow when using social network and media sites to avoid the potential for problems.

1. Read the privacy and acceptable use policies before joining or publishing information on a social network or social media site.
2. Avoid installing toolbars and plug-ins offered on social network or social media sites. These programs tend to slow down computers, cause technical problems and tend to gather data about you that you may not wish to share.
3. Follow best security practices to secure your account. Use a strong, different password for each site and never share this password with anyone. Use two-step or two-factor authentication on all available sites.
4. Do not share your password with anyone.
5. Use the privacy settings on a social media or social network site to only share information intentionally to the people you choose.
6. Do not publish information that you would not want your family, co-workers, supervisors, current and future employers, etc., to see.
7. Do not publish information about others that is personal, private, or protected by law on a social network.
8. Remember that others can post information about you on these sites.
9. Social networks generate most of their revenue through advertising. Do not publish information about yourself that you do not want to be used for targeted

marketing.

10. Choose your friends wisely. Avoid adding people as friends if you have not met them in person or you do not have an established relationship with them through other channels. “Friends” on social networking sites usually have access to more of your information than the casual browser.

11. Social networks are as much about relationships as they are about sharing information. Think twice before becoming a “fan” of a controversial topic, group, or person if you would not want your family, co-workers, supervisors, current and future employers to know about your support of that issue or person.

12. Avoid misrepresenting yourself or your background.

13. Remember that not everything you see or read on the Internet is true. Always be sure to check sources of information before relying on what is published on social networking and media sites.