

Online Safety

What do we mean by “online safety”?

Keeping safe online means protecting yourself from incurring some type of negative outcome as a result of your online behavior. There can be a variety of potential negative outcomes or consequences that one can experience if they are not careful about how they conduct themselves while on-line.

For example, posting personal information online can lead to

- Others accessing your information and making decisions or judgments about you, whether these judgments are accurate or not. This could include friends, coworkers, employers or schools.
- Bullying, harassment, or stalking
- Being accused of misconduct or other breach of a website or University policy
- Libelous and/or slanderous information about you displayed in a public forum online
- Fraud or identity theft

The above links provide examples of cases where the technology we take for granted resulted in negative and even dangerous consequences. Even though these instances are not common, as our reliance on technology increases, we will surely see more cases like these.

Technology is a great tool, and if it is used wisely, can be very useful and beneficial to our personal and academic lives. However, it is important to protect yourself while making use of the technology and online opportunities that are available.

Specifically, for members of an institution of higher education (students, staff, and faculty) it is important to keep in mind the following

- You are a representative and/or affiliate of your university.
- You are held accountable for any information you post and can be subjected to discipline or other actions under university policies.
- Several intellectual property and copyright issues surround research and academic work.

Why is it important to know about online safety?

- Anything you post online is
 - o Public
 - o Persistent (e.g. you leave a “Digital Footprint” or “Digital Tattoo”)
 - even if you ‘delete’ or remove information, it may be archived in cyberspace (cached on search engine servers, held on social networking site archives) and could be accessed at a later date, by audience you may not anticipate (potential employers for example).

- You are accountable for what you post
 - o Institutional jurisdiction
 - Many organizations or agencies can access this information
 - Violations of policies and procedures of these institutions, including those at the University of Manitoba, can be subject to discipline action,
- People can be harmed online in the same way that they can be harmed in person
 - o For example, email messages or web blogs can contain offensive or harassing information. Social network sites that involve posting of personal information, photos, and videos can also result in the negative outcomes described above.

Therefore, it is important that everyone know how to keep safe when using the internet and online resources. We have included some helpful tips and resource information to assist you with keeping safe online.

Specific Tips and Strategies

- o If you post content or hold an account on a social networking site, know the privacy settings and terms/conditions of that site. [Click here for information about being safe on Facebook.](#)
- o Before you post content on publicly accessible pages, consider whether you would still be posting this information if you knew it would be displayed to an audience of professors, friends, family, employers etc.
- o Be careful not to post sensitive information about yourself or others in online public sites. Examples of sensitive information include your personal phone number, your U of M student number, the name of the bank you use, or an email password.
- o Obtain permission before you post content about other people (friends etc.).
- o Try “Googling” your own name to find out what is publicly available about you online already. This will give you an idea of the content that you can have control over.
- o Become familiar with the U of M policies on student conduct.
 - o [Student Discipline Bylaw](#)
 - o Use of Computer Facilities [Policy](#) and [Procedures](#)
 - o [Computing and Network Facilities Usage Agreement in *claimid* and annual renewal](#)
 - o [Responsible Computer Usage.](#)

If you know or suspect that there has been an on-line security related incident involving you or another member of the university community, please note the following resources:

- [Security Services](#)
- [Student Advocacy](#)
- Information Services and Technology (IST)

- Misuse or abusive behavior using UofM computer accounts or facilities may be reported by email to abuse@umanitoba.ca
- IST provides the following examples of computer security related incidences:
 - Suspicions that your account is being used by someone else
 - Harassing email
 - Viruses/email hoaxes/phishing scams
 - Incidents in the open-area computer labs
 - Copyright violations

Resources and Contacts

- [Information Services and Technology](#) has created a webpage entitled *Social Networking (Facebook, Myspace, etc) Protect your privacy*.
- [Equity Services](#) is responsible for the [Respectful Work and Learning Environment Policy](#) at the University of Manitoba. This policy helps to create an environment where all members of the University community can work and study free from harassment and discrimination of any kind.
- [Student Advocacy](#) is available to assist students who need to make a complaint, or for students who have been accused of misconduct on campus.
- [Access and Privacy Coordinator's Office](#) can provide information about the policies that govern access to personal information, both electronic as well as hard-copy.



Student Advocacy
519 University Centre
University of Manitoba, Winnipeg, Manitoba, Canada R3T 2N2
Telephone: 204-474-7423 Fax: 204-474-7567
Email: student_advocacy@umanitoba.ca
umanitoba.ca/student/resource/student_advocacy

Created February 2009, modified July 2009