University of Massachusetts
UMASS Medical School

Guidelines for the Use of Social Media

DECEMBER 2012

Guidelines for the Use of Social Media

At the University of Massachusetts Worcester (UMW) we understand that social media can be a rewarding way to share your life and opinions with family, friends and colleagues around the world. Because of the great potential benefits of social media, UMW encourages the free-flow of information using these tools to advance scholarship, share knowledge, build relationships and connect with others who share similar professional and/or academic interests.

However, use of social media also presents certain risks and carries with it certain responsibilities. To assist you in making responsible decisions about your use of social media, we have established these guidelines for appropriate use of social media. These guidelines apply to all UMW faculty, staff (includes residents, fellows, and post doctoral scholars as well as contractors acting on behalf of UMW) and students.

GUIDELINES

In the rapidly expanding world of electronic communication, social media can mean many things. Social media includes all means of communicating or posting information or content of any sort on the internet, including to your own or someone else's web log or blog, journal or diary, personal web site, social networking or affinity web site, web bulletin board or a chat room, whether or not associated or affiliated with UMW, as well as any other form of electronic communication.

The same principles and guidelines found in UMW policies apply to your activities online. Ultimately, you are solely responsible for what you post online. Before creating online content, consider some of the risks and rewards that are involved. Keep in mind that any of your conduct that adversely affects your job or academic performance, the performance of fellow staff or students or otherwise adversely affects customers, patients, suppliers, or people who work on behalf of UMW or its legitimate business interests may result in disciplinary action up to and including termination.

KNOW AND FOLLOW THE RULES

Carefully read these guidelines, as well as UMW policies, procedures, and guidelines to ensure your postings are consistent with these policies as well as federal, state and local regulations. Inappropriate postings that may include discriminatory remarks, harassment, and threats of violence or similar inappropriate or unlawful conduct will not be tolerated and may subject you to disciplinary action up to and including termination.

BE RESPECTFUL

Always be fair and courteous to members of the UMW community, as well as those conducting business with UMW. Also, keep in mind that you are more likely to resolve work-related concerns by utilizing UMW internal resources rather than by posting complaints to a social media outlet. Nevertheless, if you decide to post complaints or criticism, avoid using statements, photographs, video or audio that reasonably could be viewed as malicious, obscene, threatening or intimidating, that disparage members of the UMW community, its customers, patients, suppliers, or that might constitute harassment or bullying. Examples of such conduct might include offensive posts meant to intentionally harm someone's reputation or posts that could contribute to a hostile work environment on the basis of race, color, creed, religion, gender, age, sexual orientation, gender identity and expression, genetic information, national origin, covered veteran status, disability, ancestry or any other characteristic protected by law in employment.

BE HONEST AND ACCURATE

Make sure you are always honest and accurate when posting information or news, and if you make a mistake, correct it quickly. Be open about any previous posts you have altered. Remember that the Internet archives almost everything; therefore, even deleted postings can be searched. Never post any information or rumors that you know to be false about UMW or the UMW community or people working on behalf of UMW.

POST ONLY APPROPRIATE AND RESPECTFUL CONTENT

- Do not post confidential or proprietary information about UMW, its faculty, staff, students, or clients (including patients).
- Do not create a link from your blog, website, or other social networking site to a UMW website without identifying yourself as a member of the UMW community.
- Express only your personal opinions. Never represent yourself as a spokesperson for UMW. If UMW is a subject of the content you are creating, be clear and open about the fact that you are a member of the UMW community and make it clear that your views do not represent those of the UMW community, customers, suppliers or people working on behalf of UMW. If you do publish a blog or post online related to the work you do or subjects associated with UMW make it clear that you are not speaking on behalf of UMW.
- It is best to include a disclaimer such as, "The postings on this site are my own and do not necessarily reflect the views of UMW."

USING SOCIAL MEDIA AT WORK

Refrain from using social media while on work time or on equipment we provide, unless it is UMW related. Do not use UMW email addresses to register on social networks, blogs or other online tools utilized for personal use.

RETALIATION IS PROHIBITED

UMW prohibits taking negative action against any member of the UMW community for reporting a possible deviation from these guidelines or for cooperating in an investigation. Any UMW community member who retaliates against another community member for reporting a possible deviation from these guidelines or for cooperating in an investigation will be subject to disciplinary action, up to and including termination.

MEDIA CONTACTS

Faculty, staff, and students should follow the Communications Department guidelines on speaking to the media on UMW's behalf. All media inquiries should be directed to the Communications Department.

SECURITY CONSIDERATIONS FOR SOCIAL MEDIA

Common hazards associated with using Social Media
The nature of Social Media is that people share things about themselves. People may post pictures while on vacation, talk about the things they like to do in their free time, and what they do at work. This behavior is typically without risk when it is only shared with your friends, and many people assume that is as far as their information goes; however, once posted, your information may be shared inappropriately and be irretrievable. Consider this risk when determining if your pictures contain content you do not wish to share with everyone.

Beware of your privacy settings
Appropriately controlling privacy settings can be effective as a means to ensure your personal information is not widely distributed. While your friends may appreciate seeing daily pictures of your vacation, these pictures may also be visible, for example, to someone who has an interest in breaking into your house. Seeing daily pictures taken by you in Paris can alert criminals that your house and perhaps your bank accounts are not very closely monitored while you are away.

Computers may be infected while using Social Media
Social Media incorporates many of the tools that Internet miscreants use to infect computers.

1. **Image files and graphics**
   Image files frequently show up in a browser as a simple image. Attackers can use these images to install malicious software on your computer.
2. **Facebook Games and Applications**
   As with image files, Facebook Games are written by "someone". The author could be someone who just wants to publish a fun game, and it could also be someone who wants to gather information about people who play the game. They could be gathering your keystrokes (even when you're not playing the game), or they could be trying to figure out when you are not home in order to stage a burglary.
3. **Links to other sites**
   As with Image File and Graphics, if someone posts a malicious link, a user who clicks the link is brought to the site. The user may not even notice anything and assume the link is not working although when the link is followed, malicious software could be installed on the computer.

Your privacy settings matter, and so do your friend's privacy settings
When your privacy settings allow "Friends of Friends" to see your content, your information is shared with people you may not know. Just because your friend trusts someone, does not mean that you should trust them too. It is strongly recommended that your privacy setting allow only your friends to view your content, or a selected subgroup of friends, to view your content.

Social networking providers may change privacy settings without your knowledge
Social Networking service providers may configure your settings more permissively than you would like. This is usually done as part of an "upgrade" in the service. When this is done, the result may be broader distribution of your personal information than you would like. Since providers change these settings, it is important to check your profile periodically to see if things have changed, or if new settings are available. It is also important to read any notifications your provider sends you regarding changes in their privacy practice/settings.