

Guidelines for the Use of Social Media

Prepared by: the Voices Technology and Best Practices Team

Overview

This document was originally developed to provide a set of guidelines in the use of social media applications within VOICES Community, but we believe it has wider application for the University of Michigan. The rapid growth of social media technologies combined with their ease of use and pervasiveness make them attractive channels of communication. However, these tools also hold the possibility of a host of unintended consequences. To help you identify and avoid potential issues we have compiled these guidelines. They are examples of best practices from various institutions and are intended to help you understand, from a wide range of perspectives, the implications of participation in social media.

Things to Consider When Beginning to Use Social Media

Applications that allow you to interact with others online (e.g. Facebook, MySpace, etc.) require careful consideration to assess the implications of “friending,” “linking,” “following” or accepting such a request from another person. For example, there is the potential for misinterpretation of the relationship or the potential of sharing protected information. Relationships such as faculty-student, doctor-patient, supervisor-subordinate and staff-student merit close consideration of the implications and the nature of the social interaction. The following are some guidelines to follow in these cases.

General Guidelines

Maintain Confidentiality

Do not post confidential or proprietary information about the University of Michigan, its students, its alumni or your fellow employees. Use good ethical judgment and follow university policies and federal requirements, such as the Health Insurance Portability and Accountability Act (HIPAA) of 1996 and the Family Educational Rights and Privacy Act (FERPA). Review <<http://www.uofmhealth.org/News/patient+privacy+hipaa>> for HIPAA requirements and <http://ogc.umich.edu/frequently-asked-questions/faq-student.html>>. Review <<http://spg.umich.edu/policy/601.07>> for more on your responsibility as a U-M employee.

Maintain Privacy

Do not discuss a situation involving named or pictured individuals on a social media site

without their permission. As a guideline, do not post anything that you would not present in any public forum. Additional information on the appropriate handling of student, employee and patient information can be found

at: http://www.mais.umich.edu/access/download/ja_access_compliance.pdf

Respect University Time and Property

As stated in the University’s Standard Practice Guide, university computers and work time are to be used for university-related business. It’s appropriate to post at work if your comments are directly related to accomplishing work goals, such as seeking sources for information or working with others to resolve a problem. You should participate in personal social media conversations on your own time using non-U-M computers.

Do No Harm

Let your Internet social networking do no harm to the University of Michigan or to yourself whether you’re navigating those networks on the job or off.

Understand Your Personal Responsibility.

U-M staff and faculty are personally responsible for the content they publish on blogs, wikis or any other form of user-generated content. Be mindful that what you publish will be public for a long time— protect your privacy.

Be Aware of Liability

You are responsible for what you post on your own site and on the sites of others. Individual bloggers have been held liable for commentary deemed to be copyright infringement, defamatory, proprietary, libelous, or obscene (as defined by the courts). Increasingly, employers are conducting Web searches on job candidates before extending offers. Be sure that what you post today will not come back to haunt you.

Maintain Transparency

The line between professional and personal business is sometimes blurred: Be thoughtful about your posting’s content and potential audiences. Be honest about your identity. In personal posts, you may identify yourself as a U-M faculty or staff member. However, please be clear that you are sharing your views as an individual, not as a representative of the University of Michigan.

Correct Mistakes

If you make a mistake, admit it. Be upfront and be quick with your correction. If you’re posting to a blog, you may choose to modify an earlier post—just make it clear that you have done so.

Respect Others

You are more likely to achieve your goals or sway others to your beliefs if you are constructive and respectful while discussing a bad experience or disagreeing with a concept or person.

Be a Valued Member

If you join a social network, make sure you are contributing valuable insights. Don't hijack the discussion and redirect by posting self/organizational promoting information. Self-promoting behavior is viewed negatively and can lead to you being banned from Web sites or groups.

Think Before You Post

There's no such thing as a "private" social media site. Search engines can turn up posts and pictures years after the publication date. Comments can be forwarded or copied. Archival systems save information even if you delete a post. If you feel angry or passionate about a subject, it's wise to delay posting until you are calm and clear-headed. Post only pictures that you would be comfortable sharing with the general public (current and future peers, employers, etc.).

Social Media Guidelines When Posting as an Individual

Outside of work, you are free to pursue your personal interests. However, when you might be perceived online as an agent of U-M, you need to make sure it is clear to the audience that you are not representing the position of U-M or U-M policy. While the guidelines below apply only to those instances where there is the potential for confusion about your role as a U-M agent versus personal opinion, they are good to keep in mind for all social media interactions. When posting to a social media site you should:

Be Authentic

Be honest about your identity. In personal posts, you may identify yourself as a U-M faculty or staff member. However, please be clear that you are sharing your personal views and are not speaking as a formal representative of U-M. If you identify yourself as a member of the U-M community, ensure your profile and related content are consistent with how you wish to present yourself to colleagues.

Use a Disclaimer

If you publish content to any website outside of U-M and it has something to do with the work you do or subjects associated with U-M, use a disclaimer such as this: "The postings on this site are my own and do not represent U-M's positions, strategies or opinions."¹

¹A common practice among individuals who write about the industry in which they work is to include a disclaimer on their site, usually on their "About Me" page. If you discuss higher education on your own social media site, we suggest you include a sentence similar to this: "The views expressed on this [blog, Web site] are mine alone and do not necessarily reflect the views of the University of Michigan." This is particularly important if you could be perceived to be in a leadership role at U-M.

Don't Use the U-M Logo or Make Endorsements

Do not use the U-M block M, wordmark, athletic logo or any other U-M marks or images on your personal online sites. Do not use U-M's name to promote or endorse any product, cause or political party or candidate. U-M logo and trademark guidelines can be found at: <<http://vp-comm.umich.edu/brand/>>

Take the High Ground

If you identify your affiliation with U-M in your comments, readers may associate you with the university, even with the disclaimer that your views are your own. Remember that you're most likely to build a high-quality following if you discuss ideas and situations civilly. Don't pick fights online.

Don't Use Pseudonyms

Never pretend to be someone else. Tracking tools enable supposedly anonymous posts to be traced back to their authors.

Protect Your Identity

While you should be honest about yourself, don't provide personal information that scam artists or identity thieves could use. Don't list your home address or telephone number. It is a good idea to create a separate e-mail address that is used only with social media sites.

Does it Pass the Publicity Test

If the content of your message would not be acceptable for face-to-face conversation, over the telephone, or in another medium, it will not be acceptable for a social networking site. Ask yourself, would I want to see this published in the newspaper or posted on a billboard tomorrow or ten years from now?

Respect Your Audience

Don't use ethnic slurs, personal insults, obscenity, or engage in any conduct that would not be acceptable in U-M's community. You should also show proper consideration for others' privacy and for topics that may be considered sensitive—such as politics and religion.

Monitor Comments

Most people who maintain social media sites welcome comments—it builds credibility and community. However, you may be able to set your site so that you can review and approve comments before they appear. This allows you to respond in a timely way to comments. It also allows you to delete spam comments and to block any individuals who repeatedly post offensive or frivolous comments.

Social Media Guidelines When Posting on Behalf of the University of Michigan

In addition to the general guidelines discussed above, when you are posting to a social media site on behalf of U-M you need to:

Seek Approval

Any messages that might act as the “voice” or position of the university or a school/college/unit must be approved by the university or the director of the school/college/unit or their delegate.

Be Accurate

Make sure that you have all the facts before you post. It’s better to verify information with a source first than to have to post a correction or retraction later. Cite and link to your sources whenever possible -- that’s how you build community.

Be Transparent

If you participate in or maintain a social media site on behalf of the university, clearly state your role and goals. Keep in mind that if you are posting with a university username, other users do not know you personally. They view what you post as coming from the university. Be careful and be respectful. What you say directly reflects on the university. Discuss with your supervisor the circumstances in which you are empowered to respond directly to users and when you may need approval

Be Timely

Assign an administrator who can regularly monitor postings and content. Aim for standard times for postings and updates. The recommended minimum frequency is once to twice a week. But be sure not to overload your updates. Followers will stop paying attention if you overload them with information.

Be Responsible

What you write is ultimately your responsibility. Participation in social computing on behalf of U-M is not a right but an opportunity, so please treat it seriously and with respect. If you want to participate on behalf of the university, be sure to abide by its standard practice guidelines.

Respect Others

Users are free to discuss topics and disagree with one another, but please be respectful of others’ opinions. You are more likely to achieve your goals if you are constructive and respectful while discussing a bad experience or disagreeing with a concept or person.

Be a Valued Member

If you join a social network like a Facebook group or comment on someone’s blog, make sure you are contributing valuable insights. Don’t post information about topics like U-M events or a book you’ve authored unless you are sure it will be of interest to readers. Self-promoting behavior is generally viewed negatively and can lead to you being banned from websites or groups.

Be Thoughtful

If you have any questions about whether it is appropriate to write about certain kinds of material in your role as a U-M employee, ask your supervisor before you post.

Sources:

The best practices outlined above were compiled from numerous VOICES team member perspective as well as published sources from both within the University of Michigan and externally. The following published sources are used throughout the proposed social media best practices:

- i. University of Michigan Social Media, Strategy & Guidelines: <http://socialmedia.umich.edu/strategy-guidelines/>
- ii. Grand Valley State University: <http://www.gvsu.edu/socialmedia/social-media-guidelines-3.htm>
- iii. Human Resource Executive Online: <http://www.hreonline.com/HRE/view/story.jhtml?id=282114288>

Safety and Privacy Tips for Social Media Networking

The internet is open to a world-wide audience. When using social media channels, ask yourself:

1. Did I set my privacy setting to help control who can look at my profile, personal information and photos? You can limit access somewhat but not completely, and you have no control over what someone else may share.
2. How much information do I want strangers to know about me? If I give them my cell phone number, address, email, class schedule, a list of possessions (such as my CD collection) how might they use it? With whom will they share it? Not everyone will respect your personal or physical space.
3. Is the image I’m projecting by my materials and photos the one I want my current and future friends to know me by? What does my profile say to potential faculty members/advisors? Future graduate school/internship interviewers? Potential employers? Neighbors? Family? Parents? Which doors am I opening and which am I closing?
4. What if I change my mind about what I post? For instance, what if I want to remove something I posted as a joke or to make a point? Have I read the social

networking site's privacy and caching statements? Removing material from network caches can be difficult. Posted material can remain accessible on the internet until you've completed the prescribed process for removing information from the caching technology of one or multiple (potentially unknown) search engines.

5. Have I asked permission to post someone else's image or information? Am I infringing on their privacy? Could I be hurting someone? Could I be subject to libel suits? Am I violating network use policy or HIPAA privacy rules?
6. Does my equipment have spyware and virus protections installed? Some sites collect profile information to SPAM you. Others contain links that can infect your equipment with viruses that potentially can destroy data and infect others with whom you communicate. Remember to back up your work on an external source in case of destructive attacks.