MIDDLESEX COMMUNITY COLLEGE

Web 2.0/Social Media Guidelines

Engaging, Collaborating, Learning, and Sharing in Digital Environments

Information Resources Management (IRM) Committee

5/26/2010

Special thanks to Gina Hartman, Educational Technology Specialist in the Francis Howell School District, Charlene Tappan, Director of Marketing and Public Relations at Manchester Community College, and Marjorie London, Director of Labor Relations/Asst. Counsel at System Office for granting us permission to utilize their works in creating this document.

Contents

Web 2.0/Social Media Guidelines

The Middlesex Community College Information Resources Management (IRM) committee understands the importance of engaging, collaborating, learning, and sharing in digital environments within the institution of higher education. To this aim, IRM has developed the following guidelines to provide direction for Middlesex Community College (MxCC) employees when utilizing state resources to participate in online Web 2.0/social media activities. Permission of supervisor, department or division head, dean, or president should be requested before undertaking any project requiring you to establish a presence on the web using your Middlesex Community College identity.

Note: This document is meant to be a *living document*, and will be continually revised during its use.

I. General Overview

A. Definition of Web 2.0/Social Media

For purposes of this document, the terms “Web 2.0” and "social media" will refer to communication tools and platforms used for facilitating online collaboration, information sharing, and social networking. This includes, but is not limited to,:

- Blogs (ex: Blogger, Wordpress)
- Wikis (ex: PBWorks, WetPaint)
- Social networks (ex: Facebook, LinkedIn, Twitter)
- Photo, video, and presentation sharing sites (ex: YouTube, Flickr, SlideShare)
- Bookmarking sites (ex: Delicious, StumbleUpon)
- Social news sites (ex: Digg, Reddit)

MXCC or CCC management systems such as the college website and Blackboard, are not meant to be included here.

B. Purpose of Guidelines

These guidelines are being presented to encourage employees’ understanding of participation in social computing. With them we hope to foster an atmosphere of trust and individual accountability, keeping in mind that information produced by MxCC employees using CCC resources is a reflection on the college and the entire Connecticut Community Colleges system, and is subject to CCC Policies [see http://www.commnet.edu/it/policy/policies.asp].

C. Personal Responsibility

MxCC employees are personally responsible for the content they publish online. Be mindful that what you publish will be public for a long time—protect your privacy. Your online behavior should reflect the same standards of honesty, respect, and consideration that you use face-to-face.

II. Security

A. Best Practices

i. Be Aware of What You're Signing Up For

Be sure to read all information regarding ownership of content, privacy and security, etc. before signing up for an account. If the web site policies are not clear, request clarification before signing up.

ii. Never load files that contain Protected Confidential Information (PCI) Data

According to the Major Information Security Incident Response Policy [http://www.commnet.edu/it/policy/major-incident-policy.asp], PCI data is "data, which exposed to any security risk or otherwise disclosed, would violate Federal or State law or CCC contract or policy." Some examples include:

- Non-Public Directory Information
- Social Security Number, Date of Birth, or Mother's Maiden Name
- Student Loan Data
- Bank Account or Credit Card Numbers

iii. Protect Passwords

- Create strong passwords and change them regularly. [See http://www.microsoft.com/protect/fraud/passwords/create.aspx for more information.]
- Do not allow your browser to save passwords. When logging in to a Web 2.0/social media site, be sure the "Remember me" check box is turned off. Always be sure to log out when finished using the site.
- Never respond to a request to disclose your password, even if the request appears to be coming from the host site. Web 2.0/social media sites never request users to disclose passwords for any reason.

iv. Manage Security Settings

- Set up permissions and security settings within the tools/sites so that you are as confident as possible that no one can "hack" into your account and post things you would not want posted. Check these settings regularly, as sites are constantly changing and adding new features which may change security or privacy settings on pre-existing features.
- Be aware of applications/sites that ask you to "grant access" to information for second or third party sites. This happens often within an application like Facebook which has links out to many other third party applications.

v. Monitor Posts/Comments

- Post a disclaimer on your site which indicates the administrator has the right to moderate comments. Monitor postings and comments daily, and remove inappropriate postings immediately. [Refer to Section III.A.ii of this document for information on what constitutes "inappropriate postings."] Block users who cannot adhere to proper conduct.
- Respond appropriately to questions or concerns. Know ahead of time how you will address negative comments.

vi. Back Up Data

Web 2.0/social media sites can be vulnerable to hacking, server unavailability, and company shut-downs, among other issues, so it is wise to save data elsewhere. For help, refer to the following articles:

- "Free Tools to Back Up Your Online Accounts," Gina Trapani, *LifeHacker*, 12 Aug. 2009 [http://lifehacker.com/5335553/free-tools-to-back-up-your-online-accounts]
- "How to Back Up Your Social Media Accounts," Ann Smarty, *Search Engine Journal*, 9 Jan. 2010 [http://www.searchenginejournal.com/how-to-back-up-your-social-media-accounts/16117/]

B. Checking for Threats

i. How to recognize malware

Malware is designed to run undetected in the background. So how can you tell if you have undesirable software on your system? The signs to look for include:

- Advertising pop-ups that appear every few seconds
- Extra toolbars in your browser that won't go away.
- Browser going to sites you didn't tell it to go to.
- Browser settings changing so you home page won't open.
- Unexplained system slowdowns.
- Unexpected, very noticeable slowdowns in typing text into documents or into form fields.
- Sudden rise in computer crashes.

If you're experiencing these kinds of problems, it's a good idea to treat your PC as if it might be infected by checking it out thoroughly. Although there are other reasons why your system might slow down or frequently crash, if you're noticing these obvious indications of malware, your system has probably been compromised. It's time to take defensive action.

ii. How to recognize scareware

See "Scareware: FBI Warns That Those Pop-Up Security Warnings Pose a Threat to Your Computer," Paul Davis, *Business Know-How*, 5 Dec. 2008 [http://www.businessknowhow.com/security/scareware.htm]

iii. Heed the Warnings

If it looks like malware has gotten to the machine, "unplug" the network connection and call the IT Help Desk (x5711).

III. Etiquette

A. Academic Code of Conduct

Basically, the behavior of MxCC employees on Web 2.0/social media sites should reflect the same standards of honesty, respect, and consideration that are used in all aspects of college business. Important points to keep in mind:

i. Use of state resources and time

As use of state resources is restricted to state business, it follows that on-campus Web 2.0/social media use should be of a college-related, rather than personal, nature. Refer to the CT Community Colleges Board of Trustees Information Technology Resource Policy and Information Technology Acceptable Use Policy [both found at http://www.commnet.edu/it/policy/policies.asp], and the Ethical Conduct Policy of the CT Community Colleges [http://www.commnet.edu/emprel/Policy_docs/EthicalConductPolicy.doc] for more information.

ii. What is inappropriate in the classroom is inappropriate online

- Potentially offensive, discriminatory, obscene, or sexually explicit comments or images should not be posted. Definition and identification of these is up to the site administrator and their supervisor.
- Users may disagree with someone else's opinions, but should do so in a respectful way.
- Harassment and bullying is not to be tolerated.
- Existing policies governing student and employee behavior apply to the college's Web 2.0/social media presence. The college takes no responsibility for content developed or submitted by non-employees.

B. Acceptable Use

Each employee is reminded, when he or she accesses a Web 2.0/social media site with an MxCC email account, the employee is a representative of the college and should act accordingly. An employee may access such sites as Facebook to communicate with students, faculty, staff or other professional colleagues in matters related to their teaching and/or professional responsibilities, as defined in the CCC System Acceptable Use Policy.

Before using any Web 2.0/social media site for college business, employees are asked to read the site's guidelines carefully and report activities that violate any terms or conditions. Web 2.0/social media sites are an interactive tool; page administrators and college users should monitor the content closely and frequently to review user conduct. Any questionable content should be reported to a supervisor. Any content that appears threatening in any way should be reported immediately to the Dean of Finance and Administration or campus security.

i. Disclaimers

- On any site where you are (or can be) associated with MxCC, you should include a disclaimer that the views are your own and do not reflect on your employer. For example, "The postings on this site are my own and don't necessarily represent Middlesex Community College positions, strategies, or opinions."
- Instructors are encouraged to moderate content contributed by students on classroom Web 2.0/social media sites.

ii. Profiles and Identity

- Remember your association and responsibility with MxCC in online social environments. If you identify yourself as an MxCC employee, ensure your profile and related content is consistent with how you wish to present yourself with colleagues and students.
- When uploading digital pictures or avatars that represent yourself, be sure you select a college appropriate image. Any and all images should be available under Creative Commons or you should own them.

iii. Social Bookmarking

- Be aware that others can view the sites that you bookmark.
- Be aware of words used to *tag* or describe the bookmark.
- Be aware of URL shortening services and verify the landing site before submitting a link as a bookmark. (Open the link in a separate browser window by copying and pasting it in the URL address box to verify that it will go where you expect prior to pasting it into your blog, Wiki, page, etc.)
- Attempt to link directly to a page or resource if possible as you do not control what appears on landing pages in the future.

iv. Instant Messaging and Video Messaging

- MxCC employees should get authorization from their supervisor and a dean or president to have instant messaging programs and/or video messaging programs (ex: Skype) downloaded on their college computers. There are several messaging programs that are available through web interfaces with no download. MxCC employees should also recognize that use of these messaging programs should be within the guidelines of the CCC Acceptable Use Policy and request authorization prior to use.
- Profile information should follow the same guidelines as the above *Profiles and Identity* section.

v. Disciplinary Action

- Inappropriate use of Web 2.0/social media sites by users with regard to the college, its students and its staff may also lead to disciplinary action being taken. Policies regarding the acceptable use of computing resources must be adhered to. Refer to the CT Community Colleges Board of Trustees Information Technology Resource Policy [http://www.commnet.edu/it/policy/bot-computing.asp] for more information.
- The college reserves the right to request material that has been published on a Web 2.0/social media site about the college, its students or its staff that is of a questionable nature be removed from the site either by the user or by a direct request from the college to the site provider.

C. Data Privacy Issues, FERPA, and Copyright

i. FERPA

The Family Educational Rights and Privacy Act (FERPA) protects the privacy of "education records" – works created by students such as papers, projects or contributions to a web-based project. [The full text of FERPA is available at http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.] Use of Web2.0/social media tools for a class assignment may result in the disclosure of such education records. Therefore, students should provide their written consent to such possible disclosure, through the "Using Web 2.0 Technologies: Student Consent Form" [see attached document]. Alternative assignments – not posted publicly on the internet – should be made available to students who do not intend to participate in social media assignments.

ii. Intellectual Property Rights of Students

- Ownership of documents and other work products created by a user of Community College IT resources depends on the nature of the document and the identity of the creator. Works created by students are presumed to be owned by the student.
- Comments, including postings and discussions, are not considered "official records" and therefore are not subject to FERPA. (See 2002 Supreme Court decision in Owasso Independent School Dist. No. I011 v. Falvo [http://www.oyez.org/cases/2000-2009/2001/2001_00_1073] which states that peer-to-peer grading is exempt.)
- Others may not reproduce, copy or distribute student work without permission. Having students consent in writing to the sharing of their work product may be accomplished by having them sign the "Using Web 2.0 Technologies: Student Consent Form" [see attached document].

iii. Copyright

A copyright is the right to own, for a limited period of time, the exclusive right to one's work product, whether in written or other form. One need not register a work in order to own the copyright. The exclusive right of ownership is violated if someone reproduces, prepares a derivative work, distributes copies, performs or displays the work without permission from the originator.

For the use of copyright protected materials (ex: video, audio, image, documents) on a Web 2.0/social media site, written permission from the copyright holder should be submitted to the department that manages the site. Without a written consent from the copyright holder, do not store any copyright protected materials on a Web 2.0/social media site.

College- and faculty/staff-owned materials (ex: images, syllabi, websites) are considered copyright protected materials. Written permission from all copyright holders should be obtained before posting to a Web 2.0/social media site.

a. Exceptions

- "Fair use" - Under the "fair use" doctrine, small portions of a larger work. e.g., a chapter of a book, a short essay or a diagram, drawing, cartoon or picture from a book, periodical or newspaper may be used without the permission of the copyright holder. Because of the ease with which entire works may be downloaded in the online environment and saved for possible future use in violation of the creator's copyright, a number of additional restrictions apply to distance learning courses or courses using Web 2.0/social media technologies. For example, only "reasonable and limited portions" of audiovisual works or dramatic literary and musical works may be used without permission even though such works could be performed in their entirety in a classroom setting.
- "Public Domain" – A work created by another may be used without permission if the work is in the public domain. This means that the copyright has expired, which usually occurs 70 years after the creator's death. Different terms may apply to works of different authorship. All works created by employees of the federal government acting within the scope of their employment are in the public domain.
- Because of the ease with which digital content may be posted in an online course or a course using Web 2.0/social media technologies, students should be reminded that they must comply with copyright law.

Addendum

A Note on Sources

In creating this document, IRM utilized and adapted – with permission – information from the following:

- "Social Media Guidelines for Schools" [http://socialmediaguidelines.pbworks.com]. Permission obtained December 15, 2009 from Gina Hartman, Educational Technology Specialist.
- Manchester Community College's Social Networking Policy. Permission obtained December 18, 2009 from Charlene Tappan, Director of Marketing and Public Relations.
- "Legal Considerations Associated with Use of Web 2.0 Technologies" handouts distributed by Marjorie London, Director of Labor Relations/Asst. Counsel, at the "Meeting Your Students Where They Are: Building Community and Engaging Students Through Social Networking and Web 2.0" conference on 11/06/2009 at Housatonic CC.

Useful Resources

CCC Policies

- Ethical Conduct Policy of the CT Community Colleges [http://www.commnet.edu/emprel/Policy_docs/EthicalConductPolicy.doc]
- Office of Information Technology Policies [http://www.commnet.edu/it/policy/policies.asp]

Security Articles

- "Create Strong Passwords," *Microsoft Online Safety* , 2010 [http://www.microsoft.com/protect/fraud/passwords/create.aspx]
- "Free Tools to Back Up Your Online Accounts," Gina Trapani, *LifeHacker*, 12 Aug. 2009 [http://lifehacker.com/5335553/free-tools-to-back-up-your-online-accounts]
- "How to Back Up Your Social Media Accounts," Ann Smarty, *Search Engine Journal*, 9 Jan. 2010 [http://www.searchenginejournal.com/how-to-back-up-your-social-media-accounts/16117/]
- "Scareware: FBI Warns That Those Pop-Up Security Warnings Pose a Threat to Your Computer," Paul Davis, *Business Know-How*, 5 Dec. 2008 [http://www.businessknowhow.com/security/scareware.htm]

FERPA

- Family Educational Rights and Privacy Act Regulations (FERPA) [http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html]
- 2002 Supreme Court decision in Owasso Independent School Dist. No. I011 v. Falvo [http://www.oyez.org/cases/2000-2009/2001/2001_00_1073]

USING WEB 2.0 TECHNOLOGIES: STUDENT CONSENT FORM

_____
Name & year of class

_____
Name of faculty member

_____
Name of technology tool

This ***technology tool*** is for use in connection with the ***above mentioned class***. Material created by you and others will be posted on the web and will be accessible to your instructor, classmates and to members of the larger Internet community. The use of this ***technology tool*** carries with certain rights and certain responsibilities. If you accept the terms stated here, please sign, date and return a copy of this form to the ***above listed faculty member***.

Rights

As a student using this ***technology tool***, you are the owner of any original work that you reduce to tangible form. Others may not reproduce, copy or distribute your work without your permission.

You have a right to non-disclosure of your education records (anything that you create or that directly concerns you and that is maintained by the college). Your contributions to this ***technology tool*** constitute an education record. If you do not want your education records to be available to others, you should choose an alternative assignment that will not be posted publicly on the Internet. By contributing to this ***technology tool***, and not taking other options available to you, you consent to the collaborative use of this material as well as to the disclosure of it in this course and potentially for the use of future courses.

Responsibilities

You are required to use this ***technology tool*** responsibly. This includes complying with all applicable laws and policies. Copyright infringement, plagiarism, harassment or interference with the underlying technical code of this software are prohibited by law. Connecticut Community Colleges policies limit your use of college computers to authorized academic purposes. Unauthorized use of college software or hardware may result in the denial of privileges to access material over the college network. Recognizing the public nature of this ***technology tool***, it is particularly important that you conduct yourself in a courteous and appropriate manner.

Acceptance of Terms

I understand the terms of this ***technology tool*** and my rights and responsibilities associated with its use. I agree to comply with all applicable laws and policies.

_____	_____	_____
Name of student	Signature of student	Date

"Opt out"

I do not intend to participate in this ***technology tool*** and will accept an alternative assignment that is not posted publicly on the Internet.

_____	_____	_____
Name of student	Signature of student	Date