

MCG PUBLIC COMMUNICATION GUIDELINES FROM SOCIAL NETWORKING TO OPEN MIC NIGHT

GENERAL

The Medical College of Georgia is committed to building a community in which all persons can work together in an atmosphere free of harassment, exploitation, or intimidation. This commitment impacts public communications by members of the MCG community. For instance, when using MCG electronic resources to access on-line social networks, MCG community members (faculty, residents, staff, students, and volunteers) are expected to act in keeping with existing law, policy and ethics: with honesty, integrity, and respect for the rights, privileges, privacy, sensibilities, and property of others.

In addition, social networking resources, such as MySpace, Facebook, Twitter, LinkedIn and YouTube, as well as personal blogs or Web sites, are being used increasingly by faculty, residents, staff, and students and also by the Medical College of Georgia to post events and resource material. Accordingly, this document was developed to guide members of the MCG community in their public communications using online and other methods.

MCG faculty, residents, staff, students, and volunteers are not restricted from using particular online social networks and/or digital platforms. However, users must understand that any content they make public via online social networks, or otherwise, must comply with federal and state laws and regulations, MCG policies, codes and standards, as well as policies that apply to these individuals when working at other affiliated institutions, such as MCG Health, Inc.

Above all else, everyone needs to use good judgment in public communications. The following will set forth guidelines that MCG faculty, residents, staff, students and volunteers should follow for all online and other public communications in reference to the Medical College of Georgia.

LEGAL, REGULATORY AND POLICY CONSIDERATIONS

State and federal laws and regulations designed to preserve confidential or sensitive information or address communications of a criminal nature apply to virtually all types of communications. For example, laws, regulations and Institutional policies concerning HIPAA, FERPA, copyright infringement, defamation, invasion of privacy, obscenity, pornography, sexually explicit materials, sexual harassment, and stalking apply in the setting of online and other forms of communication. Users violating these laws could be subject to civil and criminal penalties, and imprisonment as well as Institutional sanctions.

Transmission of MCG intellectual property, research data, and customer data, for example, is restricted by law and Institutional policy.

In keeping with federal and state law, MCG is authorized to capture, archive, discover, and produce official communications made by MCG personnel in the scope of their work for MCG. Institutional safeguards are required to ensure secure transmission of certain electronic information as well, such as encryption. Accordingly, members of the MCG workforce and student body must use MCG authorized systems as their primary means of performing work electronically or by computer.

MCG personnel and students may use an external system as a secondary communication channel (where the primary channel supports capture and such) but must not use an external system as the sole or primary communication channel for official MCG business.

MCG BUSINESS USE

In making decisions regarding access to the Internet and use of its computers, each MCG department and school should first consider its mission, goals, and objectives.

Only MCG faculty, residents, staff, students, and volunteers authorized by their respective departments, schools, or programs may use social networking and other web sites to conduct MCG business. If authorized and in keeping with MCG policy, an employee, student, group or volunteer may post to a social network profile or other web site using the MCG name and/or logo, an MCG email address or MCG telephone number for contact purposes, or official department information, resources, calendars, and events. To obtain this required authorization, contact the Office of University Communications.

For example: the “mcgonline” YouTube videos on *MCG Orientation* are authorized lessons “designed and developed by students for students as a resource to help make their experience at MCG be the best it can be”.

MCG-SENSITIVE MATTERS

Any online transmission of proprietary or sensitive information must be coordinated in advance through the appropriate office in conjunction with the Office of Legal Affairs.

PERSONAL USE

MCG employees, students, and volunteers are accountable for how they use the campus computer network. Just like a telephone, an Internet connection does not automatically confer permission to use it for personal purposes or entertainment.

Consistent with MCG’s policy, Information Systems Security and Computer Usage, personal use of MCG electronic resources to access social networking sites is to be limited to incidental use. Incidental use must not interfere with an individual’s performance of his/her assigned job responsibilities or someone else’s job performance or compromise the functionality of the department or campus network.

Individuals or groups within the MCG community are not permitted to present personal opinions in ways that imply endorsement by MCG.

MCG telephone numbers, email addresses, and images are not to be posted on social network profiles for personal purposes. However, an academic or staff employee or volunteer or student government officer, or registered campus organization may use their MCG title for identification purposes. Individuals are not to use their MCG titles to imply endorsement, support or opposition by MCG with regard to any personal statements, including opinions or views on any issue.

Please be aware that any information, including pictures, text, audio, and video, can become the property of these external resource owners once they are posted, and can remain online permanently. Information and material often leave the control of the person who posts them as soon as they are submitted. To help gauge information appropriate to post, users must consider what information they want available to the world now and in the future. Many times potential employers, scholarship committees, graduate school admissions committees, or even potential roommates perform "background checks" by searching the Web. So, although posted material may be legal, it still could ruin potential career or personal prospects.

RISKS – SPAM, SPYWARE, AND VIRUSES

Many social networking sites collect profile information for advertising (SPAM) targeted at individuals with particular affiliations and interests. Use of the sites may increase your exposure to SPAM.

In addition, from the social networking sites or links on social networking sites, your machine or network may be exposed to spyware and viruses that may damage your operating system, capture data, or otherwise compromise your privacy. This may affect your computer and the campus network, as well as affect others with whom you communicate.

MONITORING

MCG subscribes to a service that scours social networks for comments related to MCG. This is done for public relations purposes.

Employers, organizations, and individuals do monitor and share information they find on social networks and personal Web sites. Posted information is public information. In addition, MCG has no control over the policies and practices of outside employers, organizations, or individuals concerning information published on social networks or external Web sites.

REPORTING

Non-compliance with policy or violations of law in connection with these guidelines should be reported to the appropriate institutional office.

For example: Contact the Office of Institutional Audit and Compliance, IT Security Administration, or the Office of Legal Affairs. In addition, reports may be made to MCG's anonymous Compliance Hotline at (800) 576-6623.

INVESTIGATIONS AND DISCIPLINARY ACTIONS

In response to concerns or complaints or information provided by individuals, MCG administrators may access profiles on social networks, and may use the information in informal or formal investigations or other proceedings.

SAFETY

The information you post can be used by others to harm you. Examples of criminal activity using information available online include identity theft, stalking, and harassment. Be cautious of posting any personal information. Your full name, address, birthday, pictures, hometown or even plans for the day can all be used by a criminal to target you.

Whether professionally or for incidental personal use, if you use social networks, please view and/or read the following:

- *“Social Networking Safety Tips: Maintain Your Identity, Keep Your Friends, Protect Your Data”*
http://podcaster.gcsu.edu/podcastdata/MCG/Channel_28325/podcast_19329/19329.m4v
- *“We Care Safety Tips”*
<http://www.policy.ucsb.edu/policies/advisory-docs/social-networking-we-care.pdf>
- *“10 Ways To Stay Out of Trouble When You Post to Social Networking Sites”*
<http://blogs.techrepublic.com.com/10things/?p=851>

RELATED MCG POLICIES AND RESOURCES

1 Board of Regents Policy Manual <http://www.usg.edu/policymanual/>

2 Confidentiality Statement http://www.mcg.edu/hr/MCGConfidentStatement_02-2006.pdf

3 Data Management and Classification <http://www.mcg.edu/policies/2215.html>

4 Employee Handbook http://www.mcg.edu/hr/documents/Employee_Handbook_web_6.11.08.pdf

5 Ethics Policy http://www.mcg.edu/policies/documents/EthicsPolicy_000.pdf

6 Information Systems Security and Computer Usage <http://www.mcg.edu/policies/2406.html>

7 Intellectual Property <http://www.mcg.edu/faculty/facman/policies4.html>

8 MCG and MCGHI Crack Down on Music Piracy

<http://www.mcg.edu/itss/networking/security/music-piracy.html>

9 MCG Beginners Guide to Computer Security

<http://www.mcg.edu/itss/networking/security/documents/beginnersguide.pdf>

- 9 MCG Faculty Manual** <http://www.mcg.edu/faculty/facman/index.html>
- 10 MCG Graphic Standards** <http://www.mcg.edu/UA/osc/graphics.html>
- 11 MCG Trademark Use** <http://www.mcg.edu/UA/osc/elements.html>
- 12 MCG Web Publishing Standards** <http://www.mcg.edu/web/standards/>
- 13 Non-Retaliation Policy** <http://www.mcg.edu/policies/documents/Non-RetaliationPolicyv.pdf>
- 14 Photocopying of Copyrighted Work** <http://www.mcg.edu/policies/1201C.html>
- 15 Political Activities (Administrative Policy)** <http://www.mcg.edu/policies/6006.html>
- 16 Political Activity (Faculty Manual)** <http://www.mcg.edu/aaffairs/policies/pdfs/p720.pdf>
- 17 Privacy of Health Information** <http://www.mcg.edu/policies/9002.html>
- 19 Sexual Harassment Policy** <http://www.mcg.edu/policies/2205.html>
- 18 Professional Expectations** <http://www.mcg.edu/students/ssd/professionalism.html>
- 20 Student Code of Conduct / Student Handbook**
<http://www.mcg.edu/students/handbook/documents/SelectConductCodeandProcedures2009-2010Handbook.pdf>

Other Suggested Reading:

User Agreements for Electronic Resources (see Social Networking Providers' Web sites)