Weill Cornell Medicine  
Social Media Policy (For Internal Users)

I. About the WCM Social Media Policy for Internal Users (“Policy”) 
Weill Cornell Medicine (hereinafter known as “WCM”) recognize that the use of social media provides opportunities, both business and personal, for its staff, students and faculty. The purpose of this Policy is to provide rules and guidelines in order to protect WCM’s confidential information and patient privacy, and promote compliance with WCM policies and applicable law, while allowing for academic freedom.

WCM faculty, students and staff are charged with unique roles in the areas of patient care and the advancement of medicine. Due to these responsibilities, WCM expects community members, including, but not limited to, faculty, staff and students, to use any relevant social networking websites, applications or tools in a manner that is legal, ethical and consistent with WCM’s mission of education, research and patient care.

II. Terms and Definitions 
A. For purposes of this Policy, “Social Media,” “Social Network” and/or “Platform” refers to a website or application external to WCM that permits communication and the sharing of information between people. This includes, but is not limited to, all Internet-based social networking websites (e.g., Facebook, Google Plus, LinkedIn, Twitter, etc.), blogs, chat rooms, collaborative information and publishing systems (e.g., Wikis, etc.), video and photo sharing websites (e.g., YouTube, Vimeo, Flickr, Picasa), and other websites with user-generated content. 
B. “Social Media Account” refers to any registered account on any Social Network that is being used in support of the business function or needs of any organizational unit (e.g., department, center, institute, club, etc.) at WCM.
C. “Administrators” refers to any WCM faculty, staff or student responsible for the administration of and authoring content for any Social Media Account.
D. “User” refers to a member of the WCM community, including, but not limited to, faculty, students and staff, who places postings, commentary or other content on a WCM Social Media Account or a personal Social Media forum, while identifying themselves as being affiliated with WCM.

III. Scope 
This Policy applies to all faculty, students and staff of WCM who engage in online discourse.

IV. Business Use of Social Media 
WCM regularly uses social media for business and marketing purposes under the guidance of the Office of External Affairs.
Any authorized use of Social Media must be conducted in a manner that is professional, protects the reputation and brand of WCM, and is in compliance with WCM policies, the terms of use for the Social Media website, and any applicable laws and regulations. Prohibited conduct includes, for example, use of Social Media in any way that constitutes libel, false advertising, copyright or trademark infringement, harassment, professional misconduct, or a violation of privacy rights or other rights protected under the law. See all relevant WCM policies and guidelines in Section VIII of this Policy.

Section 4.01 Social Media Administration

A. The Office of External Affairs shall oversee the institutional WCM presence on Social Networking Platforms and shall evaluate whether to launch a presence on new Platforms as they become available.

B. All Social Media Accounts that represent WCM or use the WCM institutional name and/or logo for official WCM business purposes require prior approval from and registration with the Office of External Affairs. As part of registration, WCM units will be required to complete a questionnaire relating to the Social Media Account. Social Media Accounts not used for official WCM business purposes may not use the WCM logo and may not represent WCM. Registration may be completed on the WCM intranet at http://intranet.med.cornell.edu/social.

C. Any existing Social Media Accounts that represent WCM shall be reviewed routinely for Policy compliance. Administrators will be expected to correct or modify the Social Media Accounts they are responsible for to maintain compliance with this Policy. Social Media Accounts that cannot be made compliant must be terminated.

D. WCM does not pre-screen posted social content, but it shall have the right to require removal, in its sole discretion, of any content that it considers to violate this Policy. Administrators will respond promptly to content removal requests from the Office of External Affairs. WCM does not endorse or take responsibility for content posted by third parties. See WCM Social Media Policy (For External Users) on the intranet at http://intranet.med.cornell.edu/social.

E. All policies, procedures and guidelines regarding WCM trademarks, names and symbols apply to Social Networking Accounts. The Office of External Affairs can offer guidance about how to properly use names and logos and to resolve branding and copyright/trademark issues in these venues. Before Administrators launch a Social Media Account, they should consult with External Affairs regarding questions or doubts about compliance with these policies. See the Logo Guidelines in the WCM Brande Center for more detail: http://brand.weill.cornell.edu/.

Section 4.02 Patient Privacy and The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Patient privacy is of utmost importance. The Administrator and all participants representing WCM must follow all existing WCM policies and guidelines, including WCM HR Policy 218 HIPAA and Protected Health Information, the Social Network’s User
Terms and Conditions, and routine approvals through the appropriate department, division or program.

A. Users shall not use Social Media to disclose any personally identifiable information about WCM patients in any form (including, but not limited to, any photo or video of a patient or body part), except with the patient’s written authorization on an officially sanctioned WCM-HIPAA waiver and appearance authorization form, and with the approval of the Office of External Affairs.

B. Patients receiving joint care or participating in joint research with other partner institutions, such as, but not limited to, NewYork-Presbyterian, Memorial Sloan Kettering and Hospital for Special Surgery, are protected by the patient privacy and HIPAA policies of those institutions as well. Administrators must consult with partner institutions and receive clearance before releasing personally identifiable information from such patients.

C. Personally identifiable information is defined as information that may identify the patient, including demographic information such as the patient’s name, age, address, gender, race, social security number or marital status, as well as Protected Health Information (“PHI”), which includes information that relates to a patient’s physical or mental health or condition, related health care services or payment for health care services. Even if a patient is not identified by name, a disclosure could still violate WCM or Hospital policies, HIPAA, or other applicable laws if there is a reasonable basis to believe that the patient could be identified from the disclosure.

D. Social Networks are considered open systems and may not be used to receive, discuss or transmit electronic personally identifiable information about patients. This includes private or public questions and messages to and from current or prospective patients on all Social Networks. See ITS Policy 11.3 Data Classification.

Section 4.03 Social Media for Research

Use of Social Media for clinical trial recruitment must be reviewed and approved by the WCM Institutional Review Board (IRB). Proposals for use of Social Media for this purpose should be submitted to the WCM IRB by the principal investigator through the standard protocol submission process (for example, with an initial submission or via an amendment). Written IRB approval of the proposed Social Media activity must be received prior to publicly discussing the recruiting study on Social Media and prior to requesting the assistance of External Affairs or ITS.

V. Personal and Business Conduct on Social Media

WCM respects the right of its faculty, staff, and students to use Social Media as a medium of self-expression and academic freedom, including using these media for personal interests and affiliations or other lawful purposes. When using Social Media for personal or business purposes, Users should follow the guidelines and policies set
forth herein in order to establish a clear line between their personal and WCM related activities and to protect the business and legal interests of WCM.

Section 5.01 Association with WCM

A. Users shall not use Social Media for personal purposes in any way that might reasonably create the impression that the content is authorized or controlled by WCM.

B. If Users identify themselves as being associated with WCM on a Social Media website, and if the nature or context of Social Media activity on such website could reasonably be misconstrued as representing the views of WCM, then Users should post a disclaimer such as, “My posts reflect my personal opinions and are not approved or authorized by Weill Cornell Medicine.”

C. Use of a WCM email address for Social Media purposes is use of WCM’s information system and, therefore, is covered by this Policy. WCM email addresses should be used for social networking activities only if such activities are associated with an official WCM job responsibility or academic activity. Personal Social Media Accounts should be associated with a personal email account and not a WCM email address. See WCM IT Policy 11.08 Use of Email.

D. WCM does not monitor Users’ personal accounts and is not responsible for their content.

Section 5.02 Appropriate Conduct

A. Users should always adhere to the Social Network’s user terms and conditions.

B. Use of Social Media to present information about health care topics should clarify that the content is meant for informational purposes only and not as medical advice.

C. Users should follow the WCM conflict of interest policies and declare any conflicts of interest where appropriate. If someone or some group offers to pay an employee for participating in an online forum in their WCM role, offers advertising for pay and/or for endorsement, this could constitute conflict of interest, and WCM policies and guidelines apply. See WCM’s Office of Research Integrity Conflict of Interest Policies.

D. Users should never comment on legal matters or litigation that, directly or indirectly, involves WCM. Contact the Office of External Affairs, if further assistance is required.

E. If a User is identified as associated with WCM and contacted by a member of the press, they should alert their manager and contact the Office of External Affairs before responding. External Affairs will provide assistance with this process.

F. WCM staff shall refrain from engaging in personal use of Social Media during working hours, except for limited, incidental use that does not interfere with performance of WCM duties or operations, and is compliant with WCM policies and any applicable laws and regulations. WCM community members should not expect that personal communications, including social media activities that utilize the WCM network or resources, will remain private and/or confidential. See WCM IT Policy 11.02 Privacy of the Network.
G. Users are personally responsible for their own conduct when using Social Media for personal or business purposes and should not post any content that is discriminatory, threatening or unlawful. Users are encouraged to report to the WCM Office of Human Resources any online behavior by or regarding WCM staff that violates WCM policies. See the following policies for reference: HR Policy 206 Prohibited Discrimination and Harassment, HR Policy 261 Rules of Conduct, HR Policy 262 Policies of Employee Conduct and WCM Academic Staff Handbook.

VI. Protected Activities by WCM Employees
Nothing in this Policy is intended or shall be deemed to limit the rights of WCM employees under federal or state law, including an employee’s right to discuss the terms and conditions of employment with colleagues or management or to provide information to any government agency in accordance with applicable law.

VII. Policy Management and Enforcement
Violation of this Policy may lead to disciplinary action, up to and including suspension and/or termination of employment, contract or faculty appointment. In addition, violation of HIPAA or other applicable laws or regulations may lead to the possibility of legal proceedings and/or criminal charges. Any violations of this Policy should be reported to the Office of External Affairs.

- **Responsible WCM Executives:** Vice Provost for External Affairs, Chief Information Officer, Managing Director of Human Resources and Housing
- **Responsible Departments:** Office of External Affairs, Information Technologies and Services, Office of Human Resources
- **Dates Effective:** August 31, 2014
- **Contact:** social-oversight@med.cornell.edu

VIII. Related Policies
WCM IT Policies

11.01 - Responsible Use of Information Technology Resources
11.02 - Privacy of the Network
11.03 - Data Classification
11.05 - Security Incident Response
11.07 - Copyright Infringement Policy
11.08 - Use of Email
WCM HR Policies

206 Prohibited Discrimination and Harassment
218 HIAA and Protected Health Information
261 Rules of Conduct
262 Policies of Employee Conduct

WCM Additional Policies and Guidelines

WCM Brand and Logo Guidelines
WCM Conflicts Policies at The Office of Research Integrity
WCM Academic Staff Handbook