TITLE: SOCIAL MEDIA

POLICY AND PURPOSE:

NewYork-Presbyterian Hospital recognizes that social media provide opportunities for its Hospital and medical staff, both for business and personal uses. The purpose of this policy is to provide rules and guidelines to be followed by Hospital and medical staff in order to protect the Hospital’s confidential information and patient privacy, and to promote compliance with Hospital policies and applicable law.

For purposes of this policy, social media includes but is not limited to all internet-based social networking sites (e.g., Facebook, MySpace, LinkedIn, Twitter), blogs, discussion forums, collaborative information and publishing systems (Wikis), RSS feeds, video and photo sharing websites (e.g., YouTube, Picasa) and other websites with user-generated content.

APPLICABILITY:

All Hospital Staff and Medical Staff. The terms “staff” and “users” are used interchangeably in this policy to refer to all users of social media governed by this policy.

BUSINESS USE OF SOCIAL MEDIA:

The Hospital regularly uses the Internet for business and marketing purposes under the direction of the Marketing Department. All social media content that promotes the Hospital or uses the Hospital’s brand name or logo for Hospital business purposes requires prior approval of the Marketing Department. See Hospital Policy #I258 Internet Strategy, Website/Social Media Development & Management and Hospital Policy #M110 Corporate Identification & Marketing Activities.

Any authorized use of social media must be conducted in a manner that is professional, protects the reputation and brand of the Hospital and is in compliance with Hospital policies, the terms of use for the social media site, 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.
PERSONAL USE OF SOCIAL MEDIA:

The Hospital respects the right of its staff to use social media as a medium of self-expression and does not discriminate against employees who use these media for personal interests and affiliations or other lawful purposes. When using social media for personal purposes, users should follow the guidelines and policies set forth herein in order to establish a clear line between their personal and Hospital-related activities and to protect the business and legal interests of the Hospital. In addition, Hospital 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 Hospital duties or Hospital operations and is compliant with Hospital policies and any applicable laws and regulations.

Staff 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 the Hospital, for example by placing a Hospital logo or trademark prominently on a personal Facebook page in a manner that makes the page appear to be endorsed by the Hospital. If users identify themselves as being associated with the Hospital on a social media site and if the nature or context of social media activity on such site could reasonably be misconstrued as representing the views of the Hospital, then users should post a disclaimer such as, “My posts reflect my personal opinions and are not approved or authorized by NewYork-Presbyterian Hospital.” Any social media content that promotes the Hospital, its staff or services, must be accompanied by a disclosure of the author’s relationship with the Hospital and must include the author’s actual name, not a pseudonym or alias, as required by Federal law regarding online endorsements.

Staff should remember that they are personally responsible for their own conduct when using social media for personal purposes and are discouraged from posting any content that is obscene, discriminatory, threatening or otherwise unlawful. Staff are encouraged to report to the Human Resources department any online behavior by or regarding Hospital staff that violates Hospital policies. See Code of Conduct, Employee Handbooks, Human Resources Policy #412 Harassment and Human Resources Policy #501 Equal Employment Opportunity Employment.

It is recommended that staff not communicate with, connect with or “friend” their patients or Hospital employees who directly report to them in such a manner that may inappropriately blur the personal and professional relationship, result in an invasion of privacy, or create potential liability for staff or the Hospital. It is also recommended that any use 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.
Hospital staff may not provide employment references for any current or former Hospital employees on social or professional networking sites (for example through a recommendation on LinkedIn), as such employment references could potentially be attributed to the Hospital and create legal liability for the Hospital and the author of the reference. See Human Resources Policy #503 Verification of Employment.

PATIENT PRIVACY:

Staff shall not use social media to disclose any individually identifiable information about Hospital patients in any form (including photo, video or written content) except with the patient’s written authorization on a Hospital authorization form and with the approval of the Office of Public Affairs. Individually identifiable information is 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 Hospital policies, the Health Insurance Portability and Accountability Act (HIPAA) and other applicable laws if there is a reasonable basis to believe that the patient could be identified from the disclosure. Staff are discouraged from discussing Hospital patients on social media or in any public forum, even if the patient cannot be identified. See Hospital Policy #L125 HIPAA Minimum Necessary Standard and Hospital Policy #P205 Privacy and Confidentiality/Notice of Privacy Practices.

Personal phones, personal cameras and other personal devices shall not be used to photograph, film or record Hospital patients or to receive, store or transmit individually identifiable information of Hospital patients. Staff may photograph, film or record patients using Hospital-approved equipment, but only with approval of the attending physician and with the patient’s written authorization on a Hospital authorization form. Patient authorization is not required if the photo, video or recording is taken and used solely for the purpose(s) of diagnosing, treating or identifying the patient. See Hospital Policy #P180 Photographing, Video Recording, Audio Recording of Patients and Staff and Hospital Policy #C137 Consent to Photograph, Video Record, or Audio Record for Internal Organizational Purposes.

INTELLECTUAL PROPERTY AND CONFIDENTIAL INFORMATION:

Staff shall not use social media to disclose any intellectual property or confidential information of the Hospital, its affiliates, personnel, or contractors, such as trade secrets, business plans, business agreements required by law or contract to be kept
confidential, and personal information such as an individual’s address, social security number, account number, health information or health insurance identification number.

**USE OF HOSPITAL EMAIL AND ELECTRONIC SYSTEMS AND DEVICES:**

Hospital-issued equipment and communication systems, including but not limited to the Hospital IT network, electronic mail system, computer hardware, software, tablets, laptops, telephones, cell phones, blackberries, facsimiles, and other means of electronic and telephonic communications (collectively, “electronic systems and devices”), are intended to be used for Hospital business purposes. Incidental, limited use of Hospital electronic systems or devices for personal purposes is permitted to the extent that such use does not interfere with performance of Hospital duties or Hospital operations and is fully compliant with Hospital policies and applicable laws and regulations. Hospital management may restrict access to any website, including social media sites, on select workstations.

Hospital-issued email addresses may not be used to create, register for or administer any social media or other Internet accounts, nor to post content to any Internet site, unless for Hospital business purposes. See *Hospital Policy #E115, Electronic Mail (Email).*

**NO EXPECTATION OF PRIVACY WHEN USING HOSPITAL SYSTEMS:**

All contents of Hospital electronic systems and devices are property of the Hospital. Staff shall have *no expectation of privacy* whatsoever in any data, information or communications, including social media posts, that is transmitted to, received or printed from, accessed through, stored on, or recorded on Hospital electronic systems or devices, even if for personal use. See *Hospital Policy #E115, Electronic Mail (Email)* and *Employee Handbooks.*

The Hospital reserves the right to monitor all usage of its electronic systems and to intercept, review, use, and disclose any and all aspects of its electronic systems and all files, documents, data or other information contained on or accessible through its electronic systems for any reason and at any time and without notice. Staff should not use the Hospital’s electronic systems for any personal matter that they want to keep private or confidential.
PROTECTED ACTIVITIES BY HOSPITAL EMPLOYEES:

Nothing in this policy is intended or shall be deemed to limit the rights of Hospital 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.

ENFORCEMENT:

Violation of this policy may lead to disciplinary action up to and including suspension and/or termination of employment, contract, or medical staff appointment. In addition, breach of HIPAA or other laws or regulations may lead to legal proceedings and/or criminal charges.

RELATED POLICIES:

NYP Code of Conduct
NYP Employee Handbooks
NYP Policy C137 Consent to Photograph, Video Record or Audio Record for Internal Organizational Purposes
NYP Policy E115 Electronic Mail (Email)
NYP Policy I258 Internet Strategy, Website/Social Media Development & Management
NYP Policy L125 HIPAA Minimum Necessary Standard
NYP Policy M110 Corporate Identification & Marketing Activities
NYP Policy P180 Photographing, Video Recording, Audio Recording of Patients and Staff
NYP Policy P205 Privacy and Confidentiality/Notice of Privacy Practices
HR Policy 409 Rules of Conduct (Weill Cornell/Westchester Campuses)
HR Policy 412 Harassment
HR Policy 414 Discharge for Cause (Columbia Campus)
HR Policy 501 Equal Opportunity Employment
HR Policy 503 Verification of Employment
NYP GME Policy, Use of Social Media

RESPONSIBILITY:

Vice President, Chief Marketing Officer
Senior Vice President Human Resources
POLICY DATES:

Issued: January 2012
Revised: February 2012