I. PURPOSE

The purpose of this policy is to set forth standards related to colleagues’ use of email, internet and other social media services while working at or under the direction of Loyola University Health System, any of its affiliates and/or locations.

II. DEFINITIONS/APPLICATIONS

A. Definitions

1. Colleague – for purposes of this policy, is defined as any of the following:
   a. Employees of LUMC
   b. Dually employed LUMC/LUC faculty physicians
   c. Graduate Medical Education residents and fellows

2. Users: Individuals who have been granted authorization to access, modify, delete, and/or utilize information on the LUMC Network by LUMC. Users may be colleagues, temporary staff, contractors, consultants, students, or third parties with whom special arrangements have been made.

3. E-mail: LUMC’s system for sending and receiving messages electronically over its computer network.

4. Network: A group of many interlinked local area networks and leased lines in the wide area network typically under the management of the same organization. The private communications network that is contained within an organization is called an Intranet. The main purpose of an intranet is to share company information and computing resources among colleagues.

5. Social Media is a number of web-based communication vehicles that enable users to interact with and learn from others, and to share information electronically through an organization’s intranet and Internet systems. Social Media includes, without limitation, podcasting, videocasting, blogs, discussion forums, Wiki sites and other online and network related resources, such as:
   a. Blog: A web log or website chronicling the reflections or interests of the writer.
b. Social Media Websites: On-line communications of people linked by their shared interests (e.g., YouTube, Facebook, Twitter, Pinterest, Instagram, LinkedIn, etc.).

c. Wiki: Technology that enables people to create, edit, or link to web content. Wikipedia, a free, user-written encyclopedia, is a well-known Wiki site.

d. Podcast, Videocast: A digital file distributed over a network, such as the Intranet/Internet.

e. Discussion Forums: Websites and email sites that permits Users to post questions, responses and other comments. (e.g. listserves, bulletin boards, chat rooms)

f. Misc. and New: Miscellaneous and new communication and connection services over networks to enable communications (e.g. RSS feeds, hyperlinks).

6. Network Services – For purposes of this policy, includes the definitions of Network and Social Media above (i.e., Intranet, Internet Sites and other internal communications services).

7. Protected Health Information (PHI) – Any health information that can be used to identify a patient and information related to health care operations, health care services provided to a patient, or the payment for services provided to a patient. PHI includes: 1) All medical records and other information which identifies that patient, including demographic, medical and financial information; and 2) Information in any form whether electronic, paper or spoken.

B. Applications

This policy applies to users as defined in this policy. In addition, Section 3 of this policy applies to colleagues’ online and social media activities during non-working hours whether or not they are users on the LUMC Network.

III. PROCEDURE

All Users of LUMC email and network services must use these services in an appropriate manner and protect the information on them. Users of LUMC information have the responsibility to protect that information in a manner consistent with the best interests of LUMC.

1. Acceptable Use Statements

1.1. Subject to Monitoring: LUMC reserves the right to access, monitor, or disclose, as it deems necessary, the contents and history of each user’s email messages and network services activity for any purpose. LUMC may also disclose a user’s activity and its content to law enforcement officials and/or LUMC management without the user’s consent or prior notice to the user.

1.2. Shared Accounts: Shared email and network accounts are not allowed. IDs and passwords are unique to individual users and must not be shared with other users.

1.3. Secure Confidential Information over Untrusted Networks: Information that contains confidential information or PHI that is transmitted using the Internet or other public networks must be secured. Email that stays within the LUMC network is secured and protected, however, Internet email is not secured by default and requires the user to encrypt data prior to transmission. Examples:

a. Colleague sends an email with patient information to a co-worker with an LUMC email address. This does not need to be manually encrypted by the person sending the information (i.e., user1@lumc.edu is sending an email to user2@lumc.edu).
b. Colleague wants to send an email with patient information to a contracted consulting firm. The data the colleague wants to send must be encrypted before the email may be sent (i.e., user1@lumc.edu sending an email to consultant@abcfirm.com).

1.4. **Accountable for Content:** Users are accountable for the content of their emails and for their Network use. Users should always consider whether LUMC would be comfortable if the communication was publicly disseminated.

1.5. **Appropriate Use:** It is acceptable to use the LUMC email and network services to perform your job functions. As a general matter, LUMC recognizes the use of email and network services for the following functions as appropriate to fulfill job functions:

1.5.1. Providing patient care.
1.5.2. Communicating for the purpose of conducting business.
1.5.3. Reviewing websites for product information and services.
1.5.4. Researching medical, regulatory or technical information that is appropriate to fulfill job functions.

2. **Prohibited Use**

The use of email and network services for a function that could harm the LUMC infrastructure, expose proprietary or confidential information, or create legal liabilities, or that is not appropriate to fulfill job functions, is prohibited. The following are examples of prohibited uses of the LUMC email and network services:

2.1. **Fraud and Unethical Use**

2.1.1. Misrepresenting oneself, or inappropriately representing LUMC.
2.1.2. Any misrepresentation/fraud to gain unauthorized access to a computing system or network.
2.1.3. Unauthorized decrypting or attempted decrypting of any system or user passwords or any other user’s encrypted files.
2.1.4. Using the e-mail account of another individual without express permission or proxy.
2.1.5. Solicitations that are not specifically approved by LUMC policy, administration, or department management.
2.1.6. Participating in non-LUMC sponsored contests and games, or on-line gambling.
2.1.7. Posting or mentioning identifiable LUMC patient information (i.e., PHI) through Network Services (i.e., any social media, such as Facebook).
2.1.8. Posting or mentioning of sensitive LUMC business information through Network Services.

2.2. **Service Impacting**

2.2.1. Carelessly utilizing Internet capabilities that negatively impact network performance or unduly jeopardize network computing capabilities and resources.
2.2.2. Scanning of the network is prohibited when not within the scope of one’s job function and/or specific job assignments (i.e., review of patient medical record without a specific work related reason).
2.2.3. Any unauthorized or deliberate action that damages or disrupts computing systems or networks, alters their normal performance, or causes them to malfunction regardless of location or duration.
2.2.4. Willfully introducing a computer virus, Trojan horse or other destructive program into the LUMC Network, systems or into external systems or networks.

2.2.5. Attempting to establish a separate Internet linkage or Internet service (including e-mail), or utilizing the network provided Internet utilities for unauthorized purposes, including connecting a wireless access point to the LUMC network without authorization by LUHS Information Technologies.

2.2.6. Automatically forwarding email to an external destination not specifically approved by LUMC policy, administration, or department management (i.e., forwarding an email from a LUMC email account to a personal email account (i.e., gmail, yahoo or other third party account) is not permissible.

2.2.7. Using the LUMC email or network services for chain letters or non- LUMC commercial or private endeavors not specifically approved by LUMC policy, administration, or department management.

2.2.8. Sending unsolicited mass E-mail messages, including the sending of "junk mail" or other advertising material (E-mail spam) from or over the LUMC network.

2.3. Offensive / Discriminating Behavior

2.3.1. Communications that are demeaning, defaming, harassing (including sexually), or discriminatory against any person.

2.3.2. Access, display, storage, or distribution of offensive, discriminatory, or pornographic material; is otherwise inconsistent with or in violation of the mission or values of LUMC; or that contributes to an intimidating or hostile work environment.

2.4. Disclosure of Confidential Information

2.4.1. Accessing and/or disclosing PHI or other Confidential Information that is not within the scope of one’s job function.

2.4.2. Dissemination of proprietary, strategic, confidential, private or otherwise restricted information without appropriate approvals and proper security controls.

2.5. Unauthorized Reproductions

2.5.1. Any violation of copyright or intellectual property rights laws.

3. Social Media and Online Activities Outside of LUMC

3.1. Colleagues must never post or mention identifiable LUMC patient information (i.e., PHI), or proprietary or confidential information of LUMC. This includes, but is not limited to photos, discussion or other such postings related to an individual patient’s care, our colleagues, patient care areas, business operations or other activities at LUMC facilities. LUMC policies concerning HIPAA and concerning its proprietary, confidential, and trade secret information apply with equal force to the transmission, use, or posting of such information using social media.

3.2. Colleagues may use LUMC work stations (i.e. LUMC computers) to access the internet for educational, research, business and training related purposes consistent with work responsibilities and assigned duties and responsibilities. **LUMC work stations may not be regularly used to access the internet for non-work related purposes. Access to the internet for non-work related purposes must not interfere with job duties, and/or patient care, or occur in areas visible to patients.**
3.3. Unless otherwise authorized by LUMC, do not use an LUMC email address as your primary means of identification when participating in social media. Personal email should be used for these activities.

3.4. When using social media and discussing topics where your affiliation with LUMC is known, colleagues must indicate that the views expressed are theirs alone and do not represent the views of LUMC.

4. Monitoring

4.1. Subject to Monitoring: LUMC reserves the right to access, filter and/or remove any messages or postings that it deems, in its sole discretion as it deems necessary, the contents and history of each user’s Network Communications activity. LUMC also may disclose a User’s activity and its content to law enforcement officials and LUMC management without the user’s consent or prior notice to the user.

4.2. No Expectation of Privacy: Users have absolutely no expectation of privacy in information created, sent to or from, received or stored in LUMC’s network communications services and information systems.

4.3. Egregious Use: Users shall avoid accessing or attempting to access sites that are inappropriate or offensive. Users shall avoid excessive use of email and network services for personal purposes.

4.4. Violation of Policy: A User who violates this policy may be subject to disciplinary action up to and including termination from employment (if a colleague), and/or his/her user access privileges may be suspended or terminated. Certain internet sites, such as, but not limited to those displaying pornography, pedophilia, hate literature, hacking sites, or that are otherwise so inappropriate or offensive that ANY access of these sites, or repeated attempts to access these sites, shall subject the User to immediate termination of access and/or employment in LUMC’s sole discretion.

IV. RESPONSIBLE PARTY
The President & Chief Executive Officer and, as applicable and in collaboration with the Chief Integrity Officer, shall use all necessary authority to implement this policy, enforce it, and assess its effectiveness from time to time. Questions regarding this policy should be addressed to the Chief Integrity Officer and/or his/her designee(s) at x62036.