

**MUSC – MUHA & University**  
**Social Media Guidelines**  
Revised April 2016

**Purpose:**

The purpose of these guidelines is to:

1. Outline the recommendations for internal and external participation in social media, including MUSC hosted social media and non-MUSC hosted social media in which an individual's affiliation with MUSC is known, identified or presumed.
2. Minimize the business, legal and personal risks that may arise from an individual's use of social media during working or non-working hours.
3. Protect the privacy and safety of our patients, employees and students.

**General Information**

These guidelines apply to all employees, students, physicians, volunteers, vendors, contract personnel and other associates of the MUSC enterprise, hereinafter referred to as MUSC Community. These guidelines apply to the use of social media during work and non-work hours when the person's affiliation with MUSC is identified, known or presumed. These guidelines do not apply to content unrelated to MUSC.

These guidelines apply equally to all organizational entities that comprise the MUSC enterprise ("the University"). This includes the University's academic division, the Medical University Hospital Authority, MUSC Physicians and all other entities understood to be part of the MUSC enterprise. Follow all applicable existing MUSC communications, privacy, conflict-of-interest and information security policies. For example, individuals must not share confidential, sensitive or proprietary information about MUSC and you must maintain patient, employee and student privacy. Among the policies most pertinent to this discussion are those concerning patient, employee and student confidentiality, the MUSC Acceptable Use of Computing and Telecommunications Resources Policy and policies involving photography and video and media relations.

## Your Responsibilities

- Using social media and other vehicles for sharing information falls into three categories and requires varying access controls:

Public Information	Any information that is appropriate for the public online or in a publication, including cloud-based platforms.	No access control needed.
MUSC Restricted information	Information that should not be available to the general public, but that is not subject to HIPAA or other privacy laws.	The use of unapproved external/cloud services for transmission or storage is <b>strictly prohibited due to state law.</b>
MUSC Protected information	Personally identifiable information that is subject to HIPAA or other privacy laws.	The use of unapproved external/cloud services for transmission or storage is <b>strictly prohibited.</b>

- Any MUSC Community member communicating on the Internet or via social media about MUSC or MUSC related matters should disclose his/her role at MUSC. Always use good judgment and strive for accuracy in these communications as errors and omissions reflect poorly on MUSC and may result in liability for MUSC.
- MUSC Community members should ensure personal blogging and social networking activity (i.e. accessing Facebook, Twitter, Instagram, Blogs, You Tube, etc.) do not interfere with work commitments. These activities should be restricted to official breaks. Supervisors should ensure employees only access social media sites at appropriate times and locations.
- MUSC Community members should contact the appropriate website manager if there are any questions about what is appropriate to include in a blog or social networking channel. Remember, if comments wouldn't be deemed appropriate by a manager or others at MUSC, it is unwise to post them to the Internet. Content contributed on these platforms becomes immediately searchable, shared and immediately leaves your control forever.
- MUSC Community members should be respectful and professional to fellow employees, students, professors, business partners, competitors and patients. In addition, avoid using unprofessional online personas.
- If a group or individual offers to pay an employee to participate in an online forum as a representative of MUSC, this could constitute a conflict of interest and relevant policies and guidelines would apply.
- If someone from the media or press contacts an MUSC Community member about posts made in online forums that relate to MUSC in any way, the member must alert his/her manager or contact Public Relations (843-792-7669 or woolwinh@musc.edu) before responding.
- Do not post the MUSC or MUSC Health logo unless it is specifically approved or included within another approved piece (e.g. banner ads and widgets). In addition, do not manipulate the logo to create a "new" logo.

## Official MUSC Social Media Sites and Platforms

### Internal Social Media

Because of security concerns, the use of Facebook for internal closed groups is not allowed. Anything posted on these pages leaves our internal network and transfers to Facebook's servers. Due to the highly confidential nature of our communications and potential for HIPAA violations, Facebook is no longer deemed a proper channel for these groups. Yammer is the approved social media vehicle for internal group communications.

Yammer is now MUSC's official, enterprise-wide social network. Yammer is a private and secure online environment that makes real-time communication, collaboration and sharing among faculty and staff easier and more efficient than ever before. It will consolidate the disparate methods used to communicate across the enterprise into a centralized "one stop" real-time service for MUSC communication, information sharing and collaboration. You will be able to use Yammer to subscribe to content based on your interests and responsibilities, send messages directly to groups or individuals and create public or private groups for departments, project teams or special interests. The ability to create and to opt into content-specific groups will promote more appropriate usage and improve community satisfaction with our enterprise social network. One of the big advantages of Yammer is that it combines the functionality of web forums with listservs so that members can receive and post messages via a web interface, mobile client or email in real time.

Yammer was reviewed and piloted by members of the MUSC family throughout 2015. Professional communicators and IT security experts have performed a formal review, and all endorse the implementation of Yammer across the MUSC enterprise. Yammer has also been approved by MUSC senior leadership.

The implementation of Yammer will replace current use of Facebook or other social media sites for internal information-sharing. All internal Facebook or other social media pages designed for staff or other internal communication must be terminated.

External social media methods for outside audiences will remain unaffected by this change and those groups may continue unaltered and within the constructs of the MUSC Social Media Guidelines.

MUS Community members can sign up for Yammer at [www.yammer.com](http://www.yammer.com), using their MUSC email address to access the MUSC channels.

There are two primary reasons that MUSC is mandating Yammer use for internal social network communication:

- 1) Security compliance. With Yammer coming under our Microsoft licensure agreement, we are able to provide best practice-level and legal requirements of security regarding the possibility of any sensitive or protected information being discussed in such a forum. In addition, when groups use applications such as Facebook, they are granting that application the rights to all the information that is posted there. With that in mind, it's easy to see how this could become a problem with HIPAA, sensitive or proprietary information or otherwise "insider" information.
- 2) Yammer is compliant with MUSC branding standards and promotes the opportunity to keep your "work" online persona separate from your "personal" social networking activities.

## External Social Media

Institutional representation through online social networking platforms must be initiated and authorized through the Communications Council's Social Media sub-committee (or other governing departments as indicated). To be clear, there may be no official MUSC sites or pages on YouTube, Facebook, Twitter, Instagram, Pinterest, etc., unless approved and/or developed by the Social Media sub-committee (or other official areas as indicated). All requests to establish official MUSC platforms must be submitted in writing. The request form can be found here: <http://mcintranet.musc.edu/socialmedia>

After submission to [socialmedia@musc.edu](mailto:socialmedia@musc.edu), the request will be reviewed by the Social Media Committee. Any existing sites or pages that are not registered will be reviewed and may be amended or taken down if they do not comply with official MUSC guidelines.

1. MUSC official sites on social network platforms may have pages or content areas assigned to departments, divisions or programs at MUSC. Communication guidelines apply to such pages, as well as to content maintained by the Marketing and Public Relations departments or other official areas.
2. Content owners are responsible for posting and using content in accordance with MUSC values, the MUSC code of conduct, HIPAA and other existing communications, privacy and conflict-of-interest and information security policies and procedures.
3. Content owners are responsible for monitoring and maintaining content:
  - Content must be current and accurate
  - Content owners will not engage in any communications that would not be acceptable in the MUSC organization. Users will respect copyrights and disclosures, and will not reveal proprietary financial, intellectual property, patient care or similar sensitive or private content.
  - Content owners are responsible for constantly monitoring postings to social media sites and deleting postings that do not adhere to MUSC policies.
4. MUSC ordinarily does not prohibit links to its web sites, provided any such link does not improperly connote an endorsement by or affiliation with MUSC or otherwise adversely impact any MUSC entity. No link may appear on any page or within any context containing content or materials that may be interpreted as libelous, obscene or criminal, or that infringes, otherwise violates or advocates the infringement or other violation of any third party rights.
5. In the spirit of embracing the interactive nature of online social media, MUSC welcomes user-generated content posts and replies on its pages. However, objectionable content is subject to deletion at the discretion of MUSC. Users should ensure that comments:
  - Are not profane or offensive
  - Are in context to the site or discussion thread
  - Respect the privacy of MUSC's patients, their families, staff and students. (Do not use names or readily identifiable personal specifics.)
  - Do not disclose any proprietary information.
6. Some social networking and blogging may be approved activities, typically in the context of Marketing and PR, where MUSC Community members engage in Internet conversations for work-related purposes. Such engagement on behalf of MUSC must be approved and coordinated through MUSC's Marketing and PR departments.

## Personal Social Media

1. Use a personal email address and not your MUSC email address as the primary means of identification. Just as an employee or student would not use MUSC stationery for a letter to the editor expressing personal views, do not use an MUSC email address to express personal views on a social networking platform or external website.
2. Write in the first person. Where a connection to MUSC is apparent, the MUSC Community member should make it clear that he/she is not speaking on behalf of MUSC. In social networking profiles, members should include this disclaimer in the "About Me" section of a blog or social networking profile: "The views expressed on this [Twitter, Facebook, blog, website] are my own and do not reflect the views of my employer/school."
3. If an MUSC Community member's personal blog, postings or other online activities are inconsistent with or would negatively impact MUSC's reputation or brand, he/she should not refer to MUSC or identify a connection to MUSC.
4. MUSC's Marketing and PR departments should be notified by MUSC Community members who use personal websites, blogs, Facebook pages, Twitter accounts, etc., that present them in their MUSC roles. These activities are encouraged if representations of MUSC are positive and the previous guidelines are followed. As previously noted, MUSC Community members should not disparage MUSC or disclose confidential information obtained through their work in these types of online communications.

*Cloud computing is the use of computing resources through the internet allowing individuals to mobilize work effort. Through cloud computing, work performed at the office can be accessed at home or on the go via any internet-connected device. The freedom of cloud services is the ability to access information from any computer or device. Cloud-based solutions have become popular due to mobility features as well as allowing users to collaborate on projects and view results in real-time.*

### **Approved Cloud Services:**

Box for MUSC – [musc.box.com](http://musc.box.com)

Skydrive (changing to OneDrive) – part of Microsoft license

### **Unapproved Cloud Services:**

*(includes but is not limited to)*

- Dropbox
- iCloud
- Google Drive
- Apple iCloud
- Amazon Cloud Drive

*If you have questions about any platform, please verify approved services via the OCIO Help Desk at 2-9700*

### **Guidelines for creating an approved MUSC social media channel:**

Fill out the request form for your proposed channel(s). Submit a separate form for each channel.

<http://mcintranet.musc.edu/socialmedia/>

Provide as much information as possible about the target audience you wish to reach. Members of the Communications Council Social Media sub-committee may contact you for additional information about your request.

Do not open new social media channels until your request has been approved.

### **Social Media Training:**

If you are interested in further social media training, please contact us via email at:

[socialmedia@musc.edu](mailto:socialmedia@musc.edu)

Several short training modules have been developed that may be helpful. Additionally, members of the Social Media Subcommittee are available for consultation based on your needs.

Any questions or correspondence should also be directed to [socialmedia@musc.edu](mailto:socialmedia@musc.edu)