Social Media Provision

Definitions

- **Administrator**: employee assigned to update and monitor the social media account
- **Blog**: an online “journal” consisting of longer entries than on other social media platforms, often focused on a single topic or person, combination of the words “web log"
- **Facebook**: currently the most popular social media site, used for both social and professional networking, can support pictures and video
- **LinkedIn**: professional social networking site used to connect with current and former coworkers, colleagues, and classmates; many uses for Human Resources, can post job vacancies
- **Malware**: short for “malicious software,” software designed to infiltrate or damage a computer system without the owner's informed consent
- **Phishing**: the criminally fraudulent process of attempting to acquire sensitive information such as usernames, passwords and credit card details by masquerading as a trustworthy entity in an electronic communication
- **Post**: (n.) content entry or update on a social media platform; (v.) to add or update content on a social media platform
- **RSS**: allows users to stay up-to-date with multiple works through a “reader” which aggregates feeds from many sites into one place, most commonly translated as "Really Simple Syndication" but sometimes "Rich Site Summary"
- **Social media**: the use of technology combined with social interaction to create or co-create value; also known as Web 2.0, new media, interactive media, and social networking
- **Twitter**: social media site growing in popularity, known as a “micro-blog” because it allows a user to post updates (to “tweet”) limited to 140 characters, good for quick updates from friends, finding out the latest news, and keeping up-to-date on one’s favorite causes
- **Web 2.0**: see “Social media”
- **YouTube**: video sharing social media website
- **Pinterest**: A virtual pinboard that allows individuals to organize and share images on the web

Provision

Emerging online social media platforms are fundamentally changing the way organizations and individuals communicate. GRHealth will be using platforms such as Facebook, Twitter, LinkedIn, and YouTube, known as “Web 2.0,” to support institutional communication goals. These guidelines outline how
GRHealth as an organization will support the components of social media. Guidelines are also provided should GRHealth staff participate on such sites during non-working hours on personal computers. Only those employees who have written and expressed approval from Office of Communications and Marketing will have posting and viewing privileges to any social media site while at work. By accessing, viewing and/or posting any content to any social media site on the internet, the employee accepts, without limitation or qualification, the guidelines below.

Institutional Social Media Communications

Because of the emerging nature of social media platforms (e.g. Facebook, Twitter, LinkedIn, YouTube, blogs, and web feeds such as RSS), these guidelines do not attempt to cover every platform. Instead, they will be applied to those cited and to any other online platform available.

1. Institutional representation on online social media platforms can only be initiated and authorized through the GRHealth Office of Communications and Marketing department. To be clear, there can be no official GRHealth sites or pages on Facebook, Twitter, YouTube, etc., unless these are developed by or through the Office of Communications and Marketing. Any existing sites or pages will be reviewed and may be amended or taken down.

2. Official GRHealth sites on social media platforms may have pages or content areas that will be assigned by Office of Communications and Marketing to other departments, programs, or groups at GRHealth. These policies will apply to such pages as well as content maintained by the Office of Communications and Marketing.

3. Internal access to and administration of GRHealth presence on identified social media platforms will be limited to staff in the Office of Communications and Marketing. Additional access may be granted to other departments only with approval by the Office of Communications and Marketing.

4. Computers approved for access to social media sites must be configured for alternative Internet connectivity (i.e., guest network) and cannot be attached to the enterprise network.

5. Assigned administrators are responsible for posting and using content in accordance with the GRHealth Values, GRHealth Standards of Conduct, HIPAA, and other relevant policies and procedures. Among the policies most pertinent to this discussion are those concerning patient confidentiality, email and internet use, photography and video, and media relations. Postings in violation of GRHealth policies will result in disciplinary action.

6. Assigned administrators are responsible for monitoring and maintaining page content:
   a. Content must be current and accurate.
   b. Administrators will not engage in communications that would not be
acceptable in the GRHealth workplace, will respect copyrights and disclosures, and will not reveal proprietary financial, intellectual property, patient care, or similar sensitive or private content.

c. Administrators are responsible for regularly monitoring external postings to social media sites, engaging with individuals who post negatively (e.g., a complaint about services), and deleting posts which are offensive or distasteful in nature.

7. Should an incident occur as a result of GRHealth presence on social media sites, the details of the incident will be brought before a panel made up of but not exclusive to representatives from Legal/Risk, Office of Communications and Marketing, Privacy and Security, and Human Resources for response and remediation.

Employee Social Media Communications

While access to social media sites from GRHealth equipment and facilities is limited to staff members of the Office of Communications and Marketing, it is recognized that GRHealth staff may participate on such sites during non-working hours on personal computers. These guidelines apply to staff using social media venues such as professional society blogs, LinkedIn, Facebook, etc. Activities which do not identify a staff member with GRHealth and are purely about personal matters would normally fall outside these guidelines.

1. GRHealth employees are encouraged to write as themselves. An employee should not discuss the organization and/or GRHealth-related matters, with the exception of assigned account administrators in the Office of Communications and Marketing and Human Resources.

2. Employees will use good judgment and strive for accuracy in communications; errors and omissions reflect poorly on GRHealth, and may result in liability for an employee or for GRHealth.

3. Employees will use a personal email address (not a “gru.edu” address) as the primary means of identification on social media platforms.

4. Employees will be thoughtful about how they present themselves as part of GRHealth in online networks. Employees will avoid using unprofessional online personas.

5. Employees will be respectful and professional.

6. Employees will follow all applicable GRHealth policies. Users are to be mindful of GRHealth values, the GRHealth Standards of Conduct, HIPAA, and other relevant policies and procedures when posting content. Among the policies most pertinent to this discussion are those concerning patient confidentiality, email and internet use, photography and video, and media relations. Postings in violation of GRHealth policies will result in disciplinary action.

7. If an employee’s blog, posting, or other online activities are inconsistent with,
or would negatively impact GRHealth’s reputation or brand, the employee must not refer to GRHealth, or identify his connection to GRHealth. In those circumstances, an employee may want to include this disclaimer: “The views expressed on this [blog, website] are my own and do not reflect the views of my employer.”

8. Employees are encouraged to contact the Office of Communications and Marketing with any questions about what is appropriate to include in one’s personal blog or social networking profile.

9. Persons connecting to, or engaging in activities involving social media sites, should be aware of the inherent risks of computer malware, viruses, and phishing scams. Computers used to connect to such sites should be maintained with current antivirus software, operating system patches, and personal firewalls.