SOCIAL NETWORKING POLICY AND GUIDELINES

BACKGROUND

Social networking sites can be an effective way to keep in touch with colleagues. Social Media sites (such as Facebook, Instagram, LinkedIn, Twitter, and YouTube) have grown in popularity and application, allowing users to post content and share it with virtually anyone. Organizations, including healthcare institutions, are rapidly integrating the use of Social Media into their education, outreach, and marketing strategies. While this creates new opportunities for communication and collaboration, it also creates vulnerabilities for individuals and institutions, especially those involved in the healthcare environment.

Without careful attention to privacy settings, anyone with access to the internet can see and share unprotected profiles, photos, and posted opinions. It is important to consider the potential impact this can have on professional individuals and organizations. This policy is adapted from UW Seattle's School of Nursing and UW Medicine's Social Networking policies and refers to the use of Social Media in clinic/patient care sites. This material is also pertinent to the School of Nursing & Health Studies (SNHS) faculty and students at all clinical sites.

PURPOSE

This document summarizes existing university policies that apply to the use of Social Media and incorporates the UW Medicine policy of limiting the use of Social Media in hospital and clinic spaces. Additionally, it outlines best practice guidelines for SNHS faculty, staff, trainees, students, and volunteers (hereafter referred to as workforce members) who participate in social networking sites and share on Social Media in other areas where use of Social Media is permitted. Social Media includes text, images, audio, and video communicated via such tools as:

- Blogs, and micro-blogs, such as Twitter
- Social networks, such as Facebook
- Professional networks, such as LinkedIn
- Video sharing sites and vlogs (video weblogs), such as You Tube
- Audio sharing, such as podcasts
- Photo sharing, such as Flickr, Photobucket, Imgur, and Instagram
- Social bookmarking, such as Pinterest and Polyvore
- Discussion Forums, such as Reddit
- Public comment sections on webpages, such as those for online news sites
- User created web pages, such as Wikipedia and other Wikis
- Any other internet-based Social Media application similar in purpose or function to those applications listed above

SECTION I: POLICY ON LIMITING USE OF SOCIAL MEDIA IN HOSPITAL AND CLINIC SPACES

Use of Social Media is prohibited while performing direct patient care activities or in work areas, unless Social Media use in these areas has been previously approved. Workforce members should limit their use of Social Media in hospital or clinic spaces to personal breaks, unless Social Media use for business purposes has been previously approved by the clinical site.

SECTION II: SUMMARY OF OTHER RELEVANT UNIVERSITY OF WASHINGTON POLICIES

1. Confidential, proprietary, and trade-secret information about The University of Washington or its affiliates, students, employees, or alumni may not be posted on Social Media. Disclosing student educational records or personally identifiable student information violates the [Family Educational Rights and Privacy Act (FERPA)](#).
2. Patient privacy must be maintained in all communications. Do not disclose information that may be used to identify patients or their health condition; and remember that even de-identified information may be recognized by patients, their families, or their employers. Disclosing confidential patient information in an inappropriate manner is a federal offense under the Health Insurance Portability and Accountability Act (HIPAA). The sanctions include significant fines and/or criminal penalties.
3. Copyright and intellectual property rights must be preserved. For comprehensive guidance, consult the [UW Copyright Connection](#). This useful site contains links to relevant laws and university policies including the [UW Patent, Invention and Copyright Policy](#) and the [Digital Millennium Copyright Act information](#). Violations may result in lawsuits, fines, and imprisonment.
4. The UW owns and controls its name(s) and other marks, logos, insignias, seal, designs, and symbols. Unauthorized use of these trademarks is prohibited by [UW trademark and licensing policies](#), and is subject to civil and criminal penalties. The UW reserves the right to assess financial penalties, issue cease and desist orders, or take other legal action.
5. Respect university time and property. The use of university computers, internet access, networks, and time on the job is subject to a number of specific rules and policies, including but not limited to the following:
   a. *As employees of Washington state agencies, faculty and staff* are subject to State law and UW policy that prohibits the use of computers and networks for most personal use except under certain circumstances. State resources may not be used to support, promote, or solicit for an outside organization or group unless otherwise provided by law and University policy, to assist an election campaign, promote or oppose a ballot proposition or initiative, or lobby the state legislature. Supervisors are responsible for monitoring the use of state resources, determining whether frequency or volume of use complies with the law, counseling staff as needed, and revoking access privileges, if necessary. See [APS 47.2: Personal Use of University Facilities, Computers, and Equipment by University Employees](#). Faculty and staff who violate published University policies regarding the personal use of University resources, facilities, computers, and equipment, or policies regarding outside work and conflict of interest are subject to appropriate

disciplinary or corrective action, including dismissal. Allegations of noncompliance with APS 47.2 are handled in accordance with [APS 47.10: Policy on Financial Irregularities and Other Related Illegal Acts](#). In addition, the state Executive Ethics Board has the authority to investigate allegations of improper use of state resources (per [RCW 42.52.360](#)), and is charged with enforcing laws and rules prohibiting state workers from improperly using state resources. The Executive Ethics Board's determinations and actions are independent of any disciplinary or corrective action taken by the university.

  b. *Student* use of computers and networks is subject to UW policies, including, but not limited to the following:
       i. [Using Your Computer in Residence Halls or connecting to the university Wi-Fi network](#)
       ii. [Chapter 478-120 WAC: UW Student Conduct Code](#)
6. In general, do not use Social Media sites for personal, non-work, related purposes when you are working or volunteering at a clinical site. Recognize that other clinical agencies or departments may also set more restrictive or specific policies regarding access to Social Media sites. When in doubt, check with your unit head.
7. Unless you are serving as an approved, official spokesperson for the university, online communications are your personal opinions and do not reflect the opinion of the University of Washington or its affiliated entities. Each workforce member is personally responsible for their posts (written, audio, video or otherwise).
8. There should be no expectation of privacy when using a University account to visit internet websites. Email communications and internet use may be subject to disclosure under the Public Records Act or for audit purposes. See [APS 47.2.2](#).
9. Adhere to the rules that apply to all other aspects of your responsibilities as a UWB SNHS workforce member, including professionalism, integrity, confidentiality, and security. Relevant University policies include, but are not limited to, the following:
       a. [UW Electronic Information Privacy Policy on Personally Identifiable Information](#)
       b. [The UW Access and Use Agreement](#)
       c. [UW Information Security policies](#)
       d. [UW Privacy Policy UW APS 2.20](#)
       e. [UW Data Management Policy](#)
       f. [UW Guidelines for Electronic Discovery](#)

SECTION III: SOCIAL NETWORKING GUIDELINES

1. **Think twice before posting**. Privacy is not a component of Social Media. Consider what could happen if a post becomes widely known and how that may reflect on both you and UWB SNHS. Search engines can turn up posts years after they are created, and comments can be forwarded or copied. If you wouldn't say it at a conference or to a member of the media, consider whether you should post it online. If you are unsure about posting something or responding to a comment, seek advice from your supervisor, residency or academic advisor, or the department head.

2. **Online anonymity is more difficult to achieve then you might think**. Most things posted online can be tracked back to the original source even if pseudonyms are used. Write everything as if you are signing it with your name.

3. **Remember your audience**. A presence in the Social Media world can easily be made available to the public at large. This includes prospective students, current students, current employers and colleagues, patients and their families, and peers. Consider the potential audience before publishing to ensure your post will not cause unintended harm or alienation.

4. **Strive for accuracy**. Check and re-check your facts before posting on Social Media. Review content for grammatical and spelling errors. This is especially important if posting on behalf of the university in any capacity.

5. **Familiarize yourself with and use conservative privacy settings, regardless of the content on your profile**. Practice restraint when disclosing personal information on social networking sites. Your information could get out to a much larger audience then you intend and compromise your safety.

6. **Consider the professional image you would like to portray**. As a rule, only post online what you would want your chair or supervisor to see. Employers are beginning to search social networking sites as part of their background checks for new employees. While we all view our lives outside of work as personal, consider the professional image you would like to portray to your patients and their families. Even seemingly innocuous pictures and comments can impact the respect and trust your patients have for you, now and in the future.

7. **Don't "friend" patients, family members or legally appointed decision makers on social networking sites. Managers should not engage in Social Media interaction with their subordinates (such as becoming "friends" on Facebook), even if a subordinate initiates the contact.**

8. **Ask permission before posting medically-related content on Social Media sites**. If you are faculty or staff, ask permission from someone with appropriate authority in your chain of command. If you are a resident or student, ask permission from someone with appropriate authority in your program.

9. **If in doubt, don't post!** It is better to be conservative then to post something that could negatively affect you now or in the future.

10. **Use disclaimer language.** If you acknowledge your UWB SNHS affiliation or you may be otherwise known or presumed to be affiliated with UWB SNHS, include disclaimers in your online communications that indicate you are not speaking officially on behalf of the organization. For example:
    a. The postings on this site are my own and do not represent the positions, strategies or opinions of my employer (or my university), or
    b. This is a personal web site, produced in my own time and solely reflecting my personal opinions. Statements on this site do not represent the views or policies of my employer, past or present, or any other organization with which I may be affiliated. All content is copyrighted.

11. **Even disclaimers are not failsafe**. Standard disclaimer language may not by itself exempt UWB SNHS managers and executives from a special responsibility when blogging. By virtue of their position, managers and executives must consider whether

personal thoughts they publish may be misunderstood as expressing UWB SNHS positions. Managers should assume that their team may read the blog.

12. **Do not harass, libel, slander, or embarrass anyone**. Do not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to another person or entity. Individuals may be held personally liable for defamatory, proprietary, or libelous commentary.

13. **Disclose your relationship to the university when making endorsements.** If you make comments that could reasonably be construed as an endorsement of UWB SNHS's services, disclose your relationship with UWB SNHS.

W UNIVERSITY *of* WASHINGTON | BOTHELL

SCHOOL OF NURSING & HEALTH STUDIES

Social Network Policy and Guidelines Agreement Form

Each Nursing student in the School of Nursing & Health Studies must sign and submit this form to CastleBranch. Please read these directions carefully, sign and upload this acknowledgement form to CastleBranch.

1. I have been provided with a copy of the School of Nursing & Health Studies Social Networking Policy and Guidelines on my CastleBranch page.

2. I have reviewed and understand the School of Nursing & Health Studies Social Networking Policies. I agree to follow the policies and guidelines as stated in the document.

Print Name: _____

Signature: _____ Date: _____

Student ID number: _____

Degree Program:
☐ RN-BSN
☐ MN