



## **Recommendation for using Social media and Electronic devices for FMS /USJ**

Social Media (spaces on the internet where users can create a profile, share/generate content, and connect with others (individuals or entities) to create a personal network or website. Examples include Facebook, Twitter, Blogger, LinkedIn, Flickr etc.). Through social media/electronic devices we share information, create content, and build meaningful social interactions, for professional and personal benefits.

Although there are immense professional benefits, inappropriate online behavior could cause major harm to professional integrity, doctor-patient and doctor-colleague relationships, future employment opportunities, and public trust and confidence in the medical profession. It may also be a violation of the existing law of the country.

As medical students, you have to maintain your professional standards whether communicating through social media or traditional media and electronic devices containing patient information. It is important to recognize that online conduct is subject to Sri Lankan laws and governed by the same laws, policies, and rules of conduct that applies to all day-to-day activities.

This guideline is to help you to use social media and electronic devices while maintaining the standards of ethical and professional conduct.

- Think carefully about publishing something on social media if you would not be comfortable having your patients/colleagues/ employers see it.
- Take care not to post images or comments that might be endorsing activities or behavior that could damage your professional reputation or be in breach of your professional obligations.
- Always verify the factual accuracy of the posts you upload on social media, whether they are written by you or when you share posts written by friends or third parties.
- Refrain from uploading offensive or derogatory posts, blogs, images, videos, false rumors or comments relating to gender, ethnicity, race, nationality, disability, gender reassignment, sexual orientation, religious basis etc.

- Never assume that you will be able to delete something completely that you have posted online as contents you post may be discoverable
- Be aware of your professional and institutional (Ex University / Hospital) social media policies. Ex: If you publish digital contents on social media using the University name, logo, or any other university intellectual property, you must follow the logo guidelines given at University Web site.
- Be aware that your personal social media activities could impact negatively on how patients, colleagues and/or others perceive you.
  - Check what your profile looks like to someone who isn't your friend and remove any photos or posts that you do not want the general public to see.
  - Before posting, always ask yourself "What would my patients/colleagues/future employers think if they saw this?" and "Would this be in breach of my employer's policies, my employment conditions and/or my obligations under the regulatory authority?"
  - If in doubt, re-evaluate your post!
- Avoid sharing identification numbers on your personal profile. These would include address, telephone numbers, passport numbers or driver's license numbers, birth date, or any other data that could be used to obtain your personal records.
- Others may post photos of you, and may "tag" you in each of the photos. It is your responsibility to make sure that these photos are appropriate and are not embarrassing or professionally compromising. It is wise to "untag" yourself from any photos as a general rule, and to refrain from tagging others unless you have explicit permission from them to do so.
- Maintain the privacy of colleagues, doctors, and other hospital employees when referring to them in a professional capacity unless they have given their permission for their name or likeness to be used.

You are responsible to protect and respect confidentiality of patients. Hence,

- Photos of patients or photos depicting the body parts of patients should not be displayed online, under any circumstances, unless specific written permission to do so has been obtained from the patient. Remember, even if you have permission, such photos may be downloadable and forwarded by others so protect patient information by de-identifying the information and/or image you post. Electronic devices containing those pictures should be kept password protected.

- Check policies about posting on social media. Even with patient consent, you may be prohibited from posting certain content by the government policies (Ex You cannot post images of any patients records)
- You may share a clinical image taken on your phone in a professional and/or closed online forum for clinical and/or educational purposes. But be aware that any material posted online, even anonymously can be traced to the original author and anything you post in a closed group can be copied and shared. Be mindful about this.
- Remember that clinical images are “health information” and must be treated with the same privacy and confidentiality as any other health record or information. Never use a clinical image in an online forum unless you have the patient’s consent to do so, or if the patient would reasonably expect you to use the image in this way, or if you are otherwise permitted by law to do so. Take precautions to prevent divulging patient identity at all times even with patient consent.
- When commenting online always be respectful. Think carefully about whether you should post anything online if you are angry or upset.
- Whenever you see content that has been posted by other doctors that may be harmful to patients or the public and/or appears unprofessional, you should bring it to the attention of the individual. If the individual is not responding, reach to your supervisors.
- Never post information which could be used for identity theft or used inappropriately by a third party.