

Social Media Guidelines

While all ECU employees are welcome to participate in social media, we encourage everyone who participates in and contributes to online commentary to understand and follow these important guidelines. Our overall goal is simple: to participate online in a respectful, relevant way that protects our reputation and follows the letter and spirit of the law and East Carolina University (ECU) policy and regulations. The keys to success in social media are being honest about who you are, being thoughtful before you post, respecting the purpose of the community where you are posting and being aware of the content of your post.

These guidelines apply to ECU employees who create or contribute to the social media environment, including but not limited to:

- Social networking sites – Facebook, MySpace, Bebo, Friendster, Inner Pirate Network
- Video and photo-sharing websites – Flickr, YouTube
- Micro-blogging sites – Twitter, Yammer
- Weblogs, including professional or academic blogs
- Forums and discussion boards - Yahoo! Groups or Google Groups
- Online encyclopedias such as Wikipedia.

1. Know the rules. Become familiar with the terms of service and policies of sites and networks in which you participate. Pay attention to updates to the terms of service. For example, Facebook's extensive terms of service are updated frequently: <https://www.facebook.com/legal/terms>.

2. Maintain confidentiality. Do not post confidential or proprietary information about ECU, its students, faculty, staff, patients or alumni. Use good ethical judgment and follow university policies and federal requirements, such as FERPA and HIPAA. As a general guideline, do not post anything that would not be available to the general public. ECU strictly prohibits the unauthorized disclosure of protected health information including patient images on any social media sites. Do not use the information you share on these sites as part of your password, and/or answers to your passphrase security questions.

3. Future Health Care Workers, Educators and Interns (e.g., Professional Programs). Maintaining confidentiality of your patient and student interactions is critical in your field. Remember not to post or share information, including photographs about these interactions. Disclosing identity, embarrassing others, and/or breaching confidentiality could jeopardize your future career. Protecting student and patient information applies to you, too. There are stiff penalties for violating this confidentiality; take guidance from the faculty and professionals in your field and safeguard information and your reputation.

4. Know the Risks. Many of the social networking sites capture information from profiles to use for advertising, which can increase the amount of SPAM you receive. In addition, viruses and spyware are distributed through links on these sites, which can increase the risk to virus and spyware exposure and threats.

5. Monitor privacy settings. Consider your audiences and be sure to restrict personal information on otherwise public sites. Choose profile photos and avatars carefully.

6. Avoid crisis situations. Never participate in social media when the topic being discussed may be considered a crisis situation. Refer all social media activity around crisis topics to ECU Police or 9-1-1.

7. Steer clear of legal matters. Never comment on anything related to legal matters, litigation or any parties ECU may be in litigation with. Refer all social media activity around legal matters to the University Attorney's office.

8. Respect university time and property. As stated in the ECU Student and Employee Computer Use Policy (www.ecu.edu/cs-itcs/policies/staffstudentpolicy.cfm) and ECU Network Use Policy (www.ecu.edu/cs-itcs/policies/networkpolicy.cfm), university computers and your work time are to be used for university-related business. It is appropriate to post at work if your comments are directly related to accomplishing work goals, such as seeking sources for information or working with others to resolve a problem. You should maintain your personal sites on your own time using non-ECU computers.

9. If you are permitted to do so, use only approved university logos. If you have been authorized by your department or unit to create a social media site or a video for posting in locations, such as YouTube, please contact University Marketing (www.ecu.edu/mktg) to inquire about using an approved logo and other images, and to ensure coordination with other ECU sites and content. The logo, seal and spirit marks represent the entire university and are reserved for use as the avatars for official university social media sites. To avoid confusion, these marks should not be used to identify individual employees using social media for personal, unit or professional communications.

10. Get recognized. If you would like to have your site listed on the Official ECU Social Media site (in development), please contact University Marketing (www.ecu.edu/mktg). The university currently maintains the following official social media sites, www.twitter/eastcarolina, www.facebook.com/pages/East-Carolina-University/105943379436633 and www.innerpirate.ning.com. We encourage departments to register their sites with University Marketing, so they are included in official university communications.

11. Be transparent and honest. If you participate in or maintain a social media site on behalf of ECU, clearly state your role and goals. Never represent yourself or ECU in a false or misleading way. All statements must be true and all claims must be substantiated. A good resource about transparency in online communities is the Blog Council's, —Disclosure Best Practices Toolkit at blogcouncil.org/disclosure.

12. Be accurate. Make sure that you have all the facts before you post. It is better to verify information with a source first than to have to post a correction or retraction later. Cite and link to your sources whenever possible; after all that is how you build community. If you make an error, correct it quickly and visibly. This will earn you respect in the online community.

13. Post thoughtful, respectful comments. You are more likely to achieve your goals or change others' opinions if you are constructive and respectful while discussing a controversial subject or disagreeing with a concept or person. Do not post spam or remarks that are off-topic or offensive.

14. Respect copyright and fair use. Always give people proper credit for their work, and make sure you have the right to use something with attribution before you publish. By using university IT resources, you are accepting that you are accessing the university-owned network, and that unauthorized or illegal use of the university network is prohibited. You are attesting that you will comply with university IT policies

located at www.ecu.edu/cs-itcs/policies, the applicable University Student and Employee Computer Use Policy at (<http://www.ecu.edu/cs-itcs/policies/staffstudentpolicy.cfm>), or Academic Computer Use Policy at (<http://www.ecu.edu/cs-itcs/policies/academicpolicy.cfm>) and other applicable university IT policies.

All users of university IT services are reminded that unauthorized downloading and sharing of music, video and software is a violation of Title 17, of the U.S. Copyright Act, Sections 504 and 505 and is punishable with civil and criminal penalties ranging from \$750 to \$250,000 and up to 10 years of imprisonment.

For more information concerning compliance with the Copyright Act, visit the U.S. Copyright Office Web site at www.copyright.gov and check out the FAQs. ECU resources are available at <http://libguides.ecu.edu/copyright> and <http://www.ecu.edu/filessharing>.

University employees who violate university computer use policies will be subject to disciplinary action as governed by policy.

Student violations are misconduct under the applicable student disciplinary code. Sanctions may include revocation of access privileges in addition to other sanctions available under the regular disciplinary procedures.

15. If it causes you to pause, then pause. Participation in social media on behalf of ECU is not a right but an opportunity, so please treat it seriously and with respect. If you are about to publish something that makes you even the slightest bit uncomfortable, review these guidelines and try to determine the cause of your hesitation. If you are still unsure, discuss it with your manager. There is no such thing as a —private social media site. Ultimately, what you publish is yours—as is the responsibility. Comments can be forwarded or copied. Archival systems save information even if you delete a post.

16. Monitor comments. Most people who maintain social media sites welcome comments—it builds credibility and community. However, you can set your site so that you can review and approve comments before they appear. This allows you to respond in a timely way to comments. It also allows you to delete spam comments and to block any individuals who repeatedly post offensive or frivolous comments.

17. Separate your personal social media sites from your professional sites. In personal posts, you may identify yourself as an ECU faculty or staff member. However, please be clear that you are sharing your views as a member of the higher education community, not as a formal representative of ECU. Do not use the ECU logo, athletic logo, or any other university marks or images on your personal online sites.

18. A common practice among individuals who write about the industry in which they work is to include a disclaimer on their site, usually on their —About Me page. If you discuss higher education on your own social media site, we suggest you include a sentence similar to this:

“The contents including all opinions and views expressed within this site, are entirely personal and do not necessarily represent the opinions or views of anyone else, including other employees in my department or at ECU. ECU has not approved and is not responsible for the material contained at this site.”

19. Take measures to protect your identity. While you want to be honest about yourself, do not provide personal information that scam artists or identity thieves could use against you. Do not

list your home address or telephone number or your work telephone or e-mail address. It is a good idea to create a separate e-mail address that is used only with your social media site.

20. Use recommended tools for instructional communication. Tools used to communicate for instruction should be limited to university-managed tools that protect student data as required by FERPA and meet guidelines for *e-discovery* (see definition below). Several university tools meet these requirements (Blackboard, Centra, Moodle).

What is E-Discovery?

The Federal Rules of Civil Procedure (FRCP) and NC State Rule of Civil Procedure govern the evidence discovery process for litigation in Federal, U.S. District and NC State Courts. Discovery is the term used for the initial phase of litigation where the parties in a dispute are required to provide each other relevant information and records, along with all other evidence related to the case. E-discovery specifies the preservation of all relevant electronic information.

To learn more about E-Discovery, see these sites:

Cornell University Law School:
www.law.cornell.edu/rules/frcp

North Carolina General Statutes Chapter 1A Rules of Civil Procedure:
law.onecle.com/north-carolina/1a-rules-of-civil-procedure/index.html

21. Be aware of location-based services and social networking applications (e.g., Facebook Places, Foursquare, Gowalla) that can “tag” files you post on the Web with confidential information you do not want to share. —Geotagging is the process of adding geographical identification to photographs, video, websites and SMS messages. Geotags are automatically embedded in pictures taken with smartphones. Most modern digital cameras do not automatically add geolocation metadata to pictures, but that is not always true. These types of services and applications can be potentially dangerous because they can allow strangers to track your movements every day, and they expose your place of work and home. To learn more about geotagging, visit en.wikipedia.org/wiki/Geotagging. The website, I Can Stalk U, (icanstalku.com/how.php#disable) provides instructions on disabling geotagging on your smartphone. Digital camera owners should study their camera’s manual to understand how to turn off GPS functions.

Recommended Reading

Best Practices for Social Media Usage in North Carolina:
www.records.ncdcr.gov/guides/best_practices_socialmedia_usage_20091217.pdf

Department of Defense (DoD) Social Media Hub:
socialmedia.defense.gov

United States Computer Emergency Readiness Team—Staying Safe on Social Network Sites:
www.us-cert.gov/cas/tips/ST06-003.html