Office of the Chief Information Security Officer
RISK ADVISORY: Social Media

ciso.uw.edu

BACKGROUND

The use of social media for University of Washington (UW) academic and business purposes creates new opportunities for communication and collaboration. UW unit-sponsored use of social media may include, but is not limited to, text, images, audio and video communicated via sites such as Facebook, Twitter, You Tube, and Flickr. Members of the UW community should be aware that UW Confidential information, including personally identifiable information, can be put at risk unless such communications are not managed appropriately or proper safeguards are not applied.

BEST PRACTICES

The Office of the Chief Information Security Officer (CISO) encourages you to be mindful of the following best practices for UW faculty, staff, and volunteers (workforce members) who engage in social media on behalf of a UW unit:

- **Privacy.** Anonymity and privacy are in a constant state of flux in the world of social media. Consider the consequences if a post becomes widely known and how it may reflect on the UW. If you are unsure about posting something or responding to a comment, seek advice from your supervisor or the unit’s executive head.

- **Authorized workforce members.** Only authorized UW workforce members should communicate via unit-sponsored social media. Units should develop clear guidelines for posting comments and personal opinions.

- **Communicate on behalf of for your unit only.** If readers see your affiliation with UW, they may read your words as representing

- **Maintain confidentiality.** Do not post UW confidential information, including personally identifiable information or protected health information. Observe all federal regulations such as FERPA and HIPAA as well as UW Administrative Policy Statements.

- **Posts and comments live a long time.** Posts and comments may be able to be found via search engine years after they are posted. Think about how a posting will reflect on your unit and the UW now and in the future.

Office of the CISO, February 2011
• **Remember your audience.** The public can easily access social media. Consider how online communication can be interpreted in many different ways by many different audiences. Office of the CISO, February 2011

• **Strive for accuracy.** Carefully review and verify your facts before posting on social media. Review content for grammatical and spelling errors. Try to cite original sources when referencing external content.

• **Privacy settings.** Where applicable, use conservative privacy settings.

• **Core Values.** Avoid posting communications that are contrary to the UW’s Core Values. Do not post any material that is obscene, defamatory, profane, libelous, threatening, harassing, abusive, hateful, or embarrassing to another individual, group, or entity. Individuals may be held personally liable for posting such material.

This list is not exhaustive. For additional information, consult your supervisor, department IT support person, marketing staff, or your unit’s executive head.

**RESOURCES**

UW Patent, Invention and Copyright Policy

Digital Millennium Copyright Act

UW trademark and licensing policies

Revised Code of Washington 42.52, Ethics in Public Service

The UW Access and Use Agreement

UW Guidelines for Electronic Discovery