Division of Information Security

Guidelines for the Use of Social Media at Penn:

I. Introduction:

Social media and its evolving platforms (e.g., Facebook, LinkedIn, X, Instagram, TikTok, etc.) play an increasingly large role in our professional lives, with its potential to better connect us and rapidly share information. The guidance below is intended to raise awareness of the immense power of social media and of best practices and policy when using social media in teaching, research, administrative work and more.

Penn recognizes the value of social media platforms for a range of business goals, including but not limited to public relations, community and donor engagement, enrollment, and talent acquisition. The University understands that it must balance its support of social media with the need to carry out its missions responsibly.

In developing this guidance and consistent with Penn's Principles of Responsible Conduct, it is also important to remember that Penn is an institution that values academic freedom, inclusion, collaboration, and respect for one another. Penn is committed to the principle of non-discrimination and does not tolerate conduct that constitutes harassment on any basis including, but not limited to, sexual, racial, ethnic, gender, religious, age, disability, sexual orientation, national origin, or gender identity harassment.

If you have further questions about these guidelines, please contact privacy@upenn.edu or security@isc.upenn.edu.

II. Penn Official Account Management

a. Conduct Penn Business on Official Penn Accounts

The conduct of Penn business should only occur on authorized Penn official social media accounts. Any posts involving Penn or any of its affiliates on personal social media accounts should be clearly labelled to avoid potential confusion.

All Penn business on Official Penn Accounts should be conducted in accordance with these guidelines and any applicable Department, School or Center social media policies or guidelines.

b. Freedom of Speech and Reservation of Rights

Penn social media accounts should promote interaction and conversation with - and between - their followers. However, there may be a point at which an audience member posts something inappropriate for the general audience. The account manager is permitted to delete user comments based on the following disclaimer, which applies to all Penn-affiliated social media accounts and is as follows:

"Penn encourages its followers, fans, and visitors to its social media accounts to interact with the University and one another freely but is not responsible for comments or posts made by visitors to or fans of Penn accounts. Comments posted by visitors and fans may not reflect official views or policies of the University. Users who make comments on social media pages should be respectful of fellow visitors and maintain civil and rational discussions. All comments are subject to social networks' terms of use and codes of conduct. Account administrators reserve the right to review all comments and posted materials and remove such materials for any reason."

While strong and reasoned discussion is permissible, Penn reserves the right to remove and/or report comments (to those platforms and to Penn administration as appropriate) that engage in false information, personal attacks (including other community members or Penn students/faculty/staff), vulgarity, or threats. The University does not permit social media messages that sell products or promote commercial or political ventures.

This disclaimer should be listed on your account's Facebook page in the About section, as well as other platforms that provide the space and your department's website. Social media audience members have a right to free speech, an account manager may only delete a comment that meets the criteria for deletion in this guidance as outlined above, but not because the manager does not like or agree with the comment.

Penn social media account managers are expected to adhere to the disclaimer as well, avoiding sharing posts that are off-topic, abusive, contain profanity, are threatening in tone, or attack someone or a group of people.

c. Authorization to Speak for the University

Before setting up a Penn account, ensure that you are properly authorized to speak for the Department, School, or Center. University Communications is the official voice of the University and should be consulted if you are in doubt about the suitability of any message reflecting on Penn.

d. Account Creation

All Penn official social media accounts should be created using a Penn departmental email address. Use a password generator to create a strong password and ensure multi-factor authentication is enabled on the account. At least two staff members should have administrative access to all social media accounts. If one of those staff members leaves Penn, appropriate transitioning and deprovisioning of account management responsibilities is required to ensure that two staff members remain with administrative access.

e. Branding

Penn branding guidelines must be followed any time the Penn logo, shield or other insignia is used. The use of the University's name, shield, logos, or other insignia for personal or non-university related purposes is prohibited and is regulated by the Office of the University Secretary.

f. Content Accessibility

Web accessibility is a shared, continuous responsibility for members of the Penn community involved in the development, creation, publishing, or sharing of digital resources. Adherence to Penn's standards ensures that electronic content is available to and usable by everyone, especially people with disabilities. For official Penn accounts, content is required to meet the accessibility standards laid out in Penn's Digital Accessibility Policy.

g. Monitoring

Penn employees who manage official Penn social media should ensure they have the time and resources to responsibly maintain and monitor the use of the social media account they oversee. This includes regular review of user groups to ensure appropriate membership and oversight of user posts. The social media account administrator(s) should also ensure that former employees or other individuals no longer have access to post content if they are no longer affiliated with Penn.

Assign an employee responsible for account content and monitoring.

h. Political/Social Opinions

Expressing political or social opinions on an official Penn social media account is prohibited as such opinions may be interpreted as official statements on behalf of the University. If you have any questions, you should consult University Communications.

i. Protect Penn Data

Protect all confidential, copyrighted, intellectual property, and proprietary information to which you have access as part of your employment at Penn when posting on official Penn official social media accounts. For example, never share the following data on personal social media sites: confidential student data (e.g., grades), patient data (e.g., health information), employee data (e.g., performance information), Social Security numbers, or other data that if exposed, could harm an individual or Penn.

When conducting Penn business, only post photos, videos, essays, or other material that Penn owns or has permission to post.

j. Online Terms

Review each social media platform's online terms to ensure they are suitable for the work you are doing. For example, some services store data in foreign countries, some respond to government requests for data without notice to users, some may use or share the data with third parties for other purposes such as targeted marketing, and some retain your data even after your account is closed. If this is a concern, you may need to explore other options, such as a service with more protective practices by default, or through an institutional agreement with Penn, or an in-house solution.

k. Stay Accurate

Penn branding guidelines must be followed any time the Penn logo, shield or other insignia is used. The use of the University's name, shield, logos, or other insignia for personal or non-university related purposes is prohibited and is regulated by the Office of the University Secretary.

Make sure facts are accurate before posting on any social media platform. Consult with University Communications as appropriate. Always review for spelling and grammar errors as this reflects on Penn.

l. Connecting with Social Media Members

Consider carefully who you "friend" and "follow" or "like" when acting on Penn's behalf on official Penn social media accounts.

m. Transparency and Endorsement

To both protect the Penn name and build trust with users, social media accounts (such as Facebook pages, Instagram profiles, etc.) that are established on behalf of Penn entities, should be explicit and accurate regarding their relationships with Penn. It must be clear to the viewer who or what Penn organization is hosting the account—this may be an individual faculty member, department, center, or School. Similarly, in keeping with Penn's non-profit purpose of education and research, social media should not be used to promote or transact any commercial business, including generating revenue from advertising, nor should any staff with administrative responsibilities realize or attempt to realize any personal monetary profit from Penn-related social media.

n. Dormant Social Media Accounts

Do not maintain dormant social media accounts bearing the Penn name. If you have created a social media account that bears the University name, Shield, Logo or other marks, and that account is not used in regular and direct support of institutional priorities, you should take steps to have the account removed from the relevant social media network.

III. Social Media and Teaching

Instructors who wish to use social media in courses should carefully consider student privacy, including compliance with the Family Educational Rights and Privacy Act (FERPA). Most information that identifies a student and is maintained by Penn, or by a Penn faculty member or agent of Penn, is protected under FERPA. This protection may extend to student postings on social media course accounts. In addition, whether or not FERPA applies, privacy risks are often significant on social media sites. As a result:

a. Instructors should use social media accounts for course-related communications only if there is a valid pedagogical reason to do so. If there is no such reason, it is recommended that student participation be optional. Instructors should also consider whether an existing trusted service, such as Canvas or other University-sponsored Course Learning Management systems, could meet the same pedagogical goal.

b. Instructors should allow students to use aliases on social media sites if it is not necessary or beneficial to the students to use their names or other identifiable information.

c. Faculty should notify students (in course descriptions and syllabi) of the use of social media in the classroom, including whether students are expected to use social media as a component of the class and whether student material will be shared with the class or with the public. They should also caution students against posting personal or sensitive material and discourage students from posting coursework for which they want to preserve their intellectual property rights.

d. Instructors should not share confidential personal data on social media sites including, without limitation, student education records (e.g., grades or coursework), patient data or other health information, employee data, or other data that if exposed, could harm an individual or Penn. e. Each social media site has Terms of Service that should be reviewed and evaluated before student and instructional material is posted. These may (and often do) contain unfavorable terms regarding privacy, security, the continued availability of the service and data, foreign and US government access, technical support, and other issues.

f. Where Penn has a formal, institutional agreement with a social media provider, many of the risks may be addressed and managed via this agreement. If you have questions about whether Penn does or can attempt to have such an agreement with a social media provider, please contact the Office of General Counsel.

IV. Social Media and Research
Penn instructors and staff should consult the IRB guidance on the use of social media in research which can be found on the IRB website.

V. Social Media and Hiring

Be cautious and use your best judgment about whether to use information found on social media sites in hiring. It is recommended that social media research be limited to publicly available information on professional platforms like LinkedIn. Social media platforms that contain information which is personal and irrelevant to the job generally should not be utilized. Also, be aware that information found online about an individual may often be inaccurate, unreliable, or out-of-date. If you need assistance with or have questions about employment policies, contact the Division of Human Resources.

VI. Social Media and Personal Safety
Social media can facilitate the useful exchange of ideas, but online discourse can also be vitriolic and lead to harassment and threats. When choosing to engage in online communications, be aware that most conversations can be read or joined by anyone. In order to limit the risk associated with online harassment, take care to avoid unintentionally revealing personal information online. Posts about your location or address, travel plans, or other potential location identifiers may pose a safety risk. Innocuous details in photos, such as bar codes on packages, buildings, and scenery, or even reflections can be used to determine addresses and locations and should be treated with caution.

Online harassment can take on different forms, such as:

a. **Doxing** is when private identifying information that is not otherwise publicly available is published online. This information can include sharing an individual's private email, personal phone number, home address, etc. on various platforms in an attempt to frighten the individual and encourage additional harassment

b. **Cyberbullying** is the willful and repeated harm inflicted through the use of computers, cell phones, and other electronic devices.

c. **Trolling** occurs when individuals deliberately follow and provoke others online, often with offensive content. While most trolling is merely a nuisance, occasionally trolling attacks can escalate to threats or to the point where numerous individuals are engaged in harassing the target and/or target's organization.

For a list of resources and ways of seeking assistance if you experience online harassment, please refer to Penn's page on Online Harassment.

If you feel unsafe for any reason or believe you have seen or read something online that may result in harm to an individual or organization, contact the Division of Public Safety at (215) 573-3333.

VII. Social Media and Tracking Technologies

When building a website, application, or other technology, Software Development Kits (SDKs), link buttons, tracking pixels, and other similar tools provided by Social Media companies may provide useful information and capabilities, like tracking information about visitors to a web page. However, these capabilities come with a risk that private information communicated by the user of the website or app may be captured by the Social Media company as well. You should contact the Privacy Office or the Office of General Counsel before enabling tracking technologies by Social Media companies on any Penn website.

VIII. Other Applicable Policies

Communications made via social media are not exempt from the expectations and obligations set forth in Penn's policies or from the laws and regulations that govern personal accountability across general and traditional forms of communication. University Policies generally can be found at upenn.edu/about/policies.

Additionally, PSOM faculty should also refer to the PSOM Faculty Social Media Policy.

IX. Additional Contacts

Penn's Office of Information Security can be reached at security@isc.upenn.edu
See also www.upenn.edu/computing/security

Penn's Division of Human Resources can be reached at (215) 898-7281
See also www.hr.upenn.edu

Penn's Division of Public Safety can be reached at (215) 573-3333.
See also www.publicsafety.upenn.edu

Penn's Office of University Communications can be reached at (215) 898-8721.
See also https://university-communications.upenn.edu

Penn's Office of the Secretary can be reached at (215) 898-7005.
See also www.secretary.upenn.edu/home

Last Updated September 19, 2024