Division of Information Security

Guidelines for the Use of Social Media at Penn:

As a University community, Penn is committed to open expression and the free exchange of ideas. Social media—such as forums, blogs, wikis, podcasts, online chats, Facebook, and Twitter—can be exciting vehicles for facilitating this kind of open expression, while also raising new questions about responsible use. Communications may occur faster and have greater permanence than an author originally intended. Messages may be rapidly forwarded or multiplied, reaching individuals beyond those intended or even known by the person posting.

And the lines between personal and professional accounts and comments may become more easily blurred.

These guidelines aim to address issues that may arise regarding the responsible use of social media in the context of Penn's teaching, research, service, and administrative functions. Because this is a rapidly changing area, we expect that new questions and guidelines may continue to arise; questions about what is permissible may also be answered in existing Penn policies and other resources, links to which are provided at the end of this document.

General:

When conducting Penn business—online and off—make sure to comply with Penn policies, including but not limited to: Copyright Policy, Acceptable Use of Electronic Resources, Non-Discrimination Policy, Sexual Harassment Policy, Solicitation and Distribution, Policy Prohibiting Workplace Violence, Confidentiality of Records, etc. You are responsible for what you post.

Because of the powerful ability of social media to broadcast information worldwide, make sure to protect all confidential, copyrighted and proprietary information to which you have access as part of your employment at Penn. For example, never share on personal social media sites such information as 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 could harm an individual.

When conducting Penn business, only post photos, videos, essays, or other material that you own or have permission to post.

Make sure that terms of the social media site 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, 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.

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:

- Instructors should use social media accounts for course-related communications only if there is a good 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 Blackboard, PennInTouch, or other University-sponsored Course Learning Management system, could meet the same pedagogical goal.
- 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.
- 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 work to which they want to preserve their intellectual property rights.
- 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.

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.

Social Media and Research:

Penn instructors and staff are strongly discouraged from using personal social media accounts in connection with research study activities involving human subjects. When possible and permitted by the Terms of Service, a separate social media account or page for the research study is advisable.

When a communication is recruiting individuals to participate in a research study or communicating study-related information to enrolled participants, a duly authorized Institutional Review Board (IRB) must approve that communication before it is posted. Penn researchers must abide by individuals' written consent, as directed and approved by a duly authorized IRB, including when social media are involved. Such consent may include whether the research subject is aware of the possible disclosure of personal information on social media sites and whether communications using social media are permitted between members of the study team and research subjects. Any communication between members of the study team and potential subjects or enrolled subjects should diligently avoid including personal information. Any and all such discussions should occur offline.

Social Media and Hiring:

Be cautious and use your best judgment about whether to use information found on social media sites in hiring. 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.

Social Media and Personal Safety:

If you believe you have seen or read something online that may result in harm to an individual or organization, apply the same judgment you would if overhearing or witnessing the event in person. For assistance identifying or preventing an event that may threaten human safety or the destruction of University property, contact the Division of Public Safety at (215) 573-3333.

Departmental and Other Organizational Accounts:

Make sure when setting up an "organizational" account that you are authorized to speak for the organization. It should be clear to the viewer what organization is hosting the account—perhaps an individual faculty member, department, center, or School. 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. 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. Make sure you have the time and resources to responsibly maintain and monitor the use of the account.