Report from C-FSC Administration & Technology Committee
Date: March 2, 2018

The subcommittee charged with drafting a best practices and guidelines document has completed its charged and produced the final draft, attached. We would like this body to ratify it. The best practices document has passed through the T-FSC and has been reviewed by Vice Provost for Educational Technology, Clay Shirky.

The members from the C-FSC of the subcommittee are as follows: Vicky Steeves, Ed Kleinert, and Antonius Wiriadjaja.

Respectfully submitted,
Vicky Steeves & Edw. Kleinert (co-chairs)

Date: February 12, 2018
To: NYU Senate Councils
From: Carol Shoshkes Reiss, Chair,
Joint Senate Committee on Administration and Technology
Re: Best Practices suggestions for course directors using software

Our committee is forwarding this document for discussion to each of the NYU Senate Councils for consideration. This set of recommendations grew out of discussions by the committee over the course of a year. *Our goals are to protect both the privacy and the intellectual property of students.*

We are requesting that your councils include discussion of the recommendations. Please inform me of your concensus. The committee will forward the recommendations to the Provost, Katherine Fleming, for implementation in courses beginning Fall, 2018. Clay Shirky, Vice Provost for Educational Technology, has already reviewed and approved this document.

Membership of joint senate committee:
T-FSC: James, Jacobs (co-chair, Law), Frank Upham (Law), Amanda Watson (Libraries), Thomas Wisniewski (Medical) & Carol Shoshkes Reiss (chair, FAS)
C-FSC: Mitchell Joachim (Gallatin), Edward Kleinert (SPS), Jung Kim (Medical) Vicky Steeves (co-chair, Libraries), Antonius Oktaviano Wiriadjaja (NYU-SH)
AMC: Norma Kenigsberg (ITS)
SSC: Jacob Abbott, Christine Dah-In Chung (NYU-AD), Karan Ganta (S18)
DC: Carol Mandel (Libraries)
Student Affairs: Craig Jolley
General Counsel's office: Mark Righter
Public Safety: Heba Nassef Gore
ITS: Kitty Bridges, Jim Robertson (also Public Affairs)

Subcommittee that drafted recommendations:
Co-chairs: Vicky Steeves, Edward Kleinert
Members: Jim Jacobs, Norma Kenigsberg, Antonius Wiriadjaja & Jim Robertson

Considerations for the Use of Social Media and non-NYU Third-Party Digital Platforms for Teaching and Learning

Purpose:

Social media provides powerful ways to communicate and have re-defined human interactions in the 21st century. When faculty assign social media use for a course, it can help engage students in expression or discussion of their ideas. However, when we require students to register for, post, upload, or otherwise communicate via a software platform not licensed by New York University, it can raise concerns about privacy, accessibility, and equity.

These risks are particularly acute considering our global university; our community members are teaching, learning, and working in nations where laws and norms are different or are interpreted differently than in the United States, and where students are often experimenting with identities and expressions in class that they would never share with the people at home.

Though faculty have the right to teach in the manner appropriate to our classes, we should assess the possible risks when we require social media use on non-NYU platforms, either as a class assignment, or in our own interactions with students. The intersection of personal and professional digital environments (aka the accounts we create from email to Amazon) creates challenges for our university members.

Faculty and staff at NYU have opportunities to use social media and third-party platforms to advance teaching, learning, and scholarship. Just as students have the right, under FERPA, to opt-out of allowing NYU to share directory information, they should have the right not to enter use of social media that generates public disclosure of their contact information or other personal details. And faculty and staff have a responsibility to ensure that the user of such services does not compromise NYU policies and values at the heart of teacher-student and mentor-mentee relationships.

These guidelines are aimed at NYU faculty and staff to guide their interactions with students, when these interactions take place on third-party platforms like Facebook, Twitter, Wikipedia, Wordpress, or Github. (Hereafter, these are referred to collectively as social media.) This can take the form of a requirement for the course itself, as with students being asked to edit something on Wikipedia or post on Instagram, or as a communications tool in the class itself, as with the use of Slack or Facebook to communicate with the students.

Faculty Responsibilities:

If a course requires students to use social media or third-party web tools, faculty should specify that at registration time, in the course description. This will minimize the disruption to any students deciding to request accommodations or decline to enroll upon hearing these expectations. The expectations should be in the form of written guidance posted on the course's class site and delivered in a soft and hard copy form to the students, ideally in the syllabus. The course syllabus is the first contact between the instructor and the learners and so sets the tone for the course. It also serves as a de facto contract between faculty and the students, so it is important that it be clear and accurate.

> **Sample Syllabus Language:**
>
> During this class, students will be required to use [list app/software] as a part of course studies, and thus, will be required to agree to the "terms of use" associated with such [app/software]. [Choose applicable sentence:] These services do not require you to create an account. *OR* These services require you to create an account, but it can be a pseudonym. *OR* These services require you to create or use an account identifying you personally.
>
> You should read carefully those terms of use regarding the impact on your privacy rights and intellectual property rights. If you have any questions regarding those terms of use or the impact on the class, you are encouraged to ask the instructor prior to enrollment.

Unless the course topic is the study of social media or third-party sites, faculty should use such sites only as secondary or tertiary channels for instruction. Students should always be given an alternative channel to access instructional content and interaction. Students should be given the option of posting under a pseudonym. (This recommendation makes it hard to use sites with 'Real Names' policies like Facebook or WeChat.) Students should not be required to create an account to view class activities on social media.

NYU-provided services (e.g., NYU Classes, NYU Box, NYU WordPress, Google Drive) have typically been vetted by NYU Office of General Counsel and NYU IT office of Policy and Compliance for privacy, FERPA, and HIPAA compliance. For instance, in 2011, NYU negotiated with Google regarding the university's use of Google Apps for Education suite (NYU Email, NYU Calendar, NYU Drive, NYU Groups, etc.), which stipulates that -- while Google can monitor traffic and usage patterns to optimize and customize the user experience -- Google will not monetize information captured in these apps (i.e., via advertising targeting and demographic sharing). Forwarding NYU email to your personal email account exposes those emails to "regular" Google Terms of Use -- with less protection than NYU has negotiated and allows the monetization of your personal data. The major risk in using social media or third-party web tools to provide instruction is the lack of such protections.

Remember: the typical business model of free social media and third-party sites is the demographics and data mining these companies conduct on their users, which they then can sell without restriction. As such, be careful when giving away your personal information to a third party, and careful about asking students to do so, as you do not know how and when this would be used.

Considerations:

The key to being safe online is common sense.

- Follow NYU IT Security updates and news -- https://wp.nyu.edu/itsecurity/
- Think through creating friend/fan/follower connections where authority relationships exist (e.g., faculty/student, boss/employee, etc.). Many times you cannot control someone sharing your content or adding you to their connections, thereby gaining visibility to your content.
- Check the default setting when using third party software. Set it to "non-public" if at all possible.
- The Terms of Service Agreement is mainly used for legal purposes by organizations which provide software or services, such as browsers, e-commerce, or search engines. A legitimate terms-of-service agreement is legally binding and may be subject to change. TOSBack.org, supported by the Electronic Frontier Foundation, lists changes in terms and policies.

As voice-based services become more popular (e.g., Siri, Amazon Echo, Facebook app on your mobile device), be aware that these services may be "always on," "listening" in the background, and sending what it hears back to corporate headquarters for analysis. Be thoughtful in requiring or recommending voice-based services as a channel for communication between/among faculty and students.

To access the internet, students and faculty at NYU global locations are urged to use a VPN or connect from an NYU campus; this provides better, safer access than from an Internet cafe or from home. Additionally, students and faculty should take care to follow best practices when scraping data from third party websites using an Application Programming Interface (API).

Individual NYU schools may offer school-based tools and services. The NYU IT Office of Information Security is available to help schools assess and vet such tools. We urge schools and individual faculty members to avail themselves of this consultation.

Scenarios:

The following examples are meant to describe the landscape where these best practices might apply:

- A student(s) is encouraged to post data about their grades, projects, past education, jobs, or written articles to an academic social networking site such as Research Gate, Academia.edu, and/or LinkedIn, which may compromise privacy and confidentiality. A faculty member may ask or try to require students to join Twitter to scrape data for classwork or to observe social connections.
- A student(s) or faculty member may need data controlled by for-profit companies for their research. Is there an agreement or 'Terms of Use' (not entered into by NYU) related to access to the data, which may impact the ability of the student or researcher to publish the findings?
- A student(s) or faculty member (or staff) is asked to establish a "friend" or "follow" between one another on social media which they may object to.
- A student(s) and/or researcher(s) using Google Glass are required to sign/accept Google's Terms of Use, which may restrict their ability to conduct and publish research and novel inventions based on this platform.
- A student(s) and/or researcher(s) may want to create a satire or parody account of real people in certain social media for their creative practice.

References & Resources:

- NYU Social Media Best Practices
- NYU Digital Respect initiative
- Education Law Insights. "Are Emails, Texts, Tweets, And Other Digital Communications Student Records Under FERPA And State Law?" February 20, 2013
- Terms of Use for NYU Google Apps for Education
- Tips from Social Media for Educators: Strategies and Best Practices
- 8 Things You Should Know Before Using Social Media in Your Course
- Learning in Bursts: Microlearning with Social Media
- FERPA and Social Media
- Is Your Use of Social Media FERPA Compliant?
- Pros and Cons of Social Media in the Classroom
- Consenting Adults? Privacy in an Age of Liberated Learning Data
- Overcoming Hurdles to Social Media in Education
- Facebook 'real name' policy stirs questions around identity