



**Date:** February 20, 2015

**Memo to:** Terrance Nolan, General Counsel and Secretary

**From:** Ann Marie Mauro  
Chairperson, N/C-Faculty Senators Council  
A/Y 2014-2015

**Subject:** N/C-Faculty Senators Council Review and Recommendations: NYU Electronic  
Communications and Social Media Policy

The N/C-Faculty Senators Council submits the attached recommendations regarding the NYU Electronic  
Communications and Social Media Policy.

**cc:** Carol Morrow, Senior Associate Provost/Chief of Staff to the Provost  
Mark Righter, Associate General Counsel

*N/C-FSC Steering Committee Members:*

Randy Mowry, N/C-FSC Vice Chairperson

Fred Carl

David Elcott, Chair N/C-FSC Taskforce on Social Media Policy

Mary Killilea

Susan Stehlik

Patrick Ying



## **N/C-FSC Recommendations regarding Electronic Communications and Social Media Policy**

The Council submits the following recommendations:

1. In response to Section II.b, “Misuses of Electronic Communications,” and its correlate references to Section IV, “Enforcement,”
  - a. We recommend an explicit articulation of the process by which a determination of violation of the Social Media Policy would be assessed, particularly in cases where “reasonability” and “unreasonability” need to be determined.
  - b. Further, determination of a violation of the Social Media Policy should be made prior to considerations provided by Section IV, “Enforcement,” by an oversight body drawn from the University Senate.
  - c. Provision granting the right to counsel shall be added that includes processes overseeing the determination of violation and Enforcement.
2. In response to Section IV.g, “Social Media and Teaching,”
  - a. We recommend students be provided a right of refusal to participate in publicly accessible and non-University administered Social Media platforms (i.e. Facebook, Twitter, etc). As these platforms are public, proprietary, require a user account, track data and user activity in a variety of electronic modes, and sell user data to third parties, Students may refuse to participate based on a range of privacy concerns, including, but not limited to, a desire not to produce a publicly networked digital footprint or concerns regarding personal stalking.
  - b. Correlate to active student participation in Social Media in the classroom and for the same reasons stated above, students need be provided a right of refusal to participate in public and non-University administered Social Media platforms in order to access course content.
3. The external social media platforms is of particular concern given that it is being used directly by the University to monitor and evaluate performance. We therefore recommend:
  - a. that the University engage in an explicit partnership, and therefore privacy and data protection agreements, with such external social media platforms, or,
  - b. the University develop its own platforms for the purpose of monitoring or evaluating performance, with an explicit and publicized set of policies regarding privacy and data retention that are in compliance with this document, or,
  - c. the University cease altogether use of external provider data collection for the purpose of performance evaluation and monitoring.

4. We recommend that any member of the University community may request and receive, within 10 days, full and complete access to any and all his or her personal and productivity data retained by the University or University partners on any of its social media platforms. This recommendation supplements Sections entitled, "Scope of Access" and "Records of Process."
5. Finally, we recommend a term-limit be placed on retention of personal and productivity data. While this may vary depending on the social media platform and requirements of state and federal law, a clearly stated "upfront" and "transparent" determination of a period of data retention shall be determined and upon expiry of such period, data shall be purged in safely and completely. This policy shall be effective in both University controlled platforms and external partners, such as Google. Furthermore, upon termination of employment or relationship to the University community, any and all data retained relating to a University community member, shall be safely and fully purged by the University, as allowed by state and federal law, at the request of the community member. This option shall be presented directly to the departing University community member as part of the relevant exit interview process.