

UNIVERSITY OF ILLINOIS
AT URBANA-CHAMPAIGN

Office of the Senate

228 English Building, MC-461
608 South Wright Street
Urbana, IL 61801-3613



SC.12.06

September 12, 2011

September 5, 2011

Dear Colleagues,

You will notice an item under Proposals for Action. This is a near final draft of the Provisional Electronic Communications Policy Document. The Senate Executive Committee has discussed this item during the past two SEC meetings. A number of suggestions were made and have been incorporated into the document. It is now ready for the full Senate to discuss. Michael Corn, Chief Privacy and Security Officer, who led the Electronic Communications Policy Team, will attend the Senate Meeting on September 12th to answer any questions you may have. Please pay particular attention to Sections 19-21. I look forward to a good discussion.

Best Wishes,

Matthew B. Wheeler
SEC Chair

Provisional Electronic Communications Policy Document

1. Audience

All members of the Campus community.

2. Scope

This policy applies to the faculty, staff, and students of the University of Illinois at Urbana-Champaign, as well as all other users of electronic communications resources provided by the Urbana campus.

3. Responsibility and Governance

The campus Chief Information Officer (CIO) is assigned the responsibility for implementing and maintaining this policy.

4. Principles

The policy enacted in this document stems from the University Code of Conduct¹. This in part states,

...those acting on behalf of the University should practice: Stewardship by exercising custodial responsibility for University property and resources;

As such all of the policy statements included here were created to provide clear guidance on the meaning of “custodial responsibility” with regard to electronic communications.

5. Policy Statements

5.1. Accessibility

All electronic communications intended to accomplish the academic and administrative tasks of the University shall be accessible to allowable users with disabilities in compliance with law and University policies. Alternate accommodations shall conform to law and University policies and guidelines.

5.2. Ownership of Copyright in Content of Electronic Communications

The ownership of copyright at the University is addressed in Article III of the General Rules of the University of Illinois, regardless of whether the work is in the content of electronic communications or fixed in some other medium. See:

<http://www.uillinois.edu/trustees/rules.cfm#art3>. This is a complex and nuanced area. The following is meant only as broad-stroke guidance and the General Rules should be consulted when resolving specific situations and deciding whether listed exceptions are applicable.

Subject to a number of exceptions specified in Article III of the General Rules, “creators retain rights to traditional academic copyrightable work.” (See General Rules, Article III Section 4a regarding Copyrights, Ownership, at <http://www.uillinois.edu/trustees/rules.cfm#sec34>.)

The University may own copyrightable works by a number of means, including, but not limited to, “works created as a specific requirement of employment or as an assigned University duty ...” and “works that are also patentable.” (See General Rules Article III, Section 4a regarding Copyrights, Ownership, at <http://www.uillinois.edu/trustees/rules.cfm#sec34> and General Rules Article III, Section 5 regarding Other Intellectual Property, Ownership, at <http://www.uillinois.edu/trustees/rules.cfm#sec35>.)

6. Allowable Uses

Electronic communications resources (accounts and equipment) are provided to meet the academic, research, and outreach mission of the University and administrative functions in support of that mission. See: <http://www.uillinois.edu/about/mission.cfm>. All standards of

¹ <http://www.ethics.uillinois.edu/policies/code.cfm>. The University Code of Conduct was approved by the Senates Conference in 2002.

behavior, courtesy, and etiquette that govern vocal and written communications also extend to electronic communications.

Restrictions. Electronic communications resources may not be used for the following:

- 6.1. illegal activities
- 6.2. activities that interfere with the mission of the University
- 6.3. commercial purposes not sanctioned by the University
- 6.4. political campaigning
- 6.5. personal use inconsistent with the guidelines provided in the Appropriate Use Policy
- 6.6. uses that violate other existing University and campus policies

7. Personal Use

The General Rules of the University of Illinois at Article V, Section 3 (see <http://www.uillinois.edu/trustees/rules.cfm#sec53>), prohibit private use of University property and services. Personal use of electronic communication resources and University resources in general is addressed in the following policies.

- *The Appropriate Use Policy, Campus Administrative Manual, Article VIII, Section 1.1:* <http://www.cam.illinois.edu/viii/VIII-1.1.htm>
- *Guidelines for Sponsorships and Advertisements, Campus Administrative Manual, Article III, Section 21:* <http://www.cam.illinois.edu/iii/iii-21.htm>
- *The Information Security Policy, Campus Administrative Manual, Article 8, Section 1.2:* <http://www.cam.illinois.edu/viii/VIII-1.2.htm>
- *Guidelines Concerning Use of University Resources for Political Campaign Activities, Campus Administrative Manual, Article VIII, Section 1.3:* <http://www.cam.illinois.edu/viii/VIII-1.3.htm>

8. Massmail and similar uses of Electronic Communications

- 8.1. Any **unsolicited** e-mail or electronic message concerning official University business which is distributed to more than one hundred faculty, staff, or students must be approved by an administrative officer whose scope of responsibility includes all the persons in the selected group. For example, a dean may approve an e-mail to all students or staff within that dean's college, or a faculty member may send messages to everyone in a course they teach. Professional communication staff (such as the campus communications officers) operate under delegated authority from their unit head.
- 8.2. No e-mail lists of more than one hundred faculty, staff, or students will be provided to any entity external to the campus unless addressed by contract, required by law, by state or federal regulation, or by a collective bargaining agreement or other contract with the Board of Trustees.

9. Unsolicited Communications

Unsolicited targeted messaging for purposes only peripherally related to the academic or administrative function of the University must support an opt-out mechanism. Examples of messages that must support an opt-out mechanism are athletics or alumni information. Examples of messages that are not obligated to support an opt-out mechanism are life-safety, academic, or employment related information.

10. Allowable Users

- 10.1. University students, faculty, staff, and others affiliated with the University (including those in program, contract, or license relationships with the University) may, as authorized by the Chancellor, be eligible to use University electronic communications resources and services for purposes detailed in the section 6 above, "Allowable Uses".

10.2. Members of the public may be granted access to electronic communication resources in support of the mission of the University for the purposes detailed above, as authorized by the Offices of the Chancellor or Provost. When granted to members of the public, electronic communications resources shall be used in accordance with existing University policies, standards, and procedures.

10.3. Access to specific electronic communications resources vary by the type of authorized user and the service provider. Some of this is spelled out at the following websites:

- *Appropriate Use Policy, Campus Administrative Manual, Article VIII, Section 1.1 at <http://www.cam.illinois.edu/viii/VIII-1.1.htm>*
- *CIO Authorized Users at the University of Illinois at Urbana-Champaign and Service Grid, <http://www.cio.illinois.edu/policies/servicegrid/index.html>*
- *Institutional Benefits for Retired Faculty and Staff, Campus Administrative Manual, Article IX, Section F4 at <http://www.cam.illinois.edu/ix/ix-e&f/ix-f-4.htm>*
- The Information Security Policy also contains an access control policy that is applicable to all forms of electronic communications. See Campus Administrative Manual, Article Viii, Section 1.2: <http://www.fs.uiuc.edu/cam/cam/viii/viii-1.2.html>

11. Endorsements and Representation (Use of the University's Name) in Electronic Communications

Individual users (student, staff, or faculty) are not permitted to benefit personally or benefit others through accepting sponsorships, acknowledging sponsorships, accepting advertisements, or advertising in University supported media (including print, broadcast, or the Internet) under any circumstances. The requirements for units are more nuanced. The policy governing these two areas is *Guidelines for Sponsorships and Advertisements*. See Campus Administrative Manual, Article III, Section 21: <http://cam.illinois.edu/iii/iii-21.htm>. For the campus identity standards (addressing the proper representation of the campus and University) see Illinois Identity Standards: <http://identitystandards.illinois.edu/>.

12. False Identity and Anonymous Communications

12.1. Individuals and units are required to accurately and correctly identify themselves in all electronic communications. In this context a “correct identity” is one that can be validated through public, University-provided directories. This is addressed in §4.iii(c) of the Appropriate Use Policy and §1-302(n) (3) of the Student Code. This policy requirement does allow for the use of “avatars” and related pseudonyms provided these can be correlated to an individual.

See:

- *Appropriate Use Policy, Campus Administrative Manual, Article VIII, Section 1.1 at <http://www.cam.illinois.edu/viii/VIII-1.1.htm>*
- *Student Code at <http://admin.illinois.edu/policy/code>*

12.2. Individuals in professional communications roles may post on behalf of a unit when third-party technological limitations exist that prevent strict adherence to this element of policy, e.g., posting to Facebook.

12.3. Exempt from this requirement are systems designed to be anonymous for the sake of reporting legal or policy infractions. For example, the Crime Stoppers TIPS service or the Dean of Student's Report Intolerance site:
<http://www.odos.illinois.edu/tolerance/reporting.asp>

13. Privacy

The University is committed to protecting the privacy of electronic communications under its control. Access to the content of electronically stored information may only be permitted through the procedure described in §VI.B of the campus Appropriate Use Policy. Nevertheless, individuals should operate under the assumption that anything put into a University account or University operations taking place within a private account *may* become public.

Information and data maintained in electronic media on University computer systems are protected by the same laws and policies, and are subject to the same limitations, as information and communications in other media. Before storing or sending confidential or personal information, campus users should understand that most materials on University systems are, *by definition*, public records. As such, they are subject to laws and policies that may compel the University to disclose them. The privacy of materials kept in electronic data storage and electronic mail is neither a right nor is it guaranteed.

Under the Illinois Freedom of Information Act (FOIA), electronic files are treated in the same way as paper files. The documents in the files of employees of the State of Illinois, including email or other stored electronic communications, are generally considered to be public documents, and may be subject to inspection through FOIA. In such cases, the campus Freedom of Information Officer must inspect files to determine which portions may be exempt from disclosure.

See:

- Freedom of Information Act (FOIA) Requests, Campus Administrative Manual, Article III, Section 1.1: <http://www.cam.illinois.edu/iii/iii-1.1.htm>
- *Appropriate Use Policy, Campus Administrative Manual, Article VIII, Section 1.1:* <http://www.cam.illinois.edu/viii/VIII-1.1.htm>

Faculty and staff should be aware that electronic communications, such as email, sent to or through third parties (particularly to private email accounts) in most cases will not be protected by University policies or processes and may be subject to exposure and use inappropriate for confidential information.

14. Security

In accordance with the Appropriate Use Policy and the Information Security Policy, individuals are obligated to maintain the confidentiality and integrity of electronic communications such as email in compliance with University and campus policies and standards. This obligation is attached to the information and thus applies to University information stored on personally-owned equipment. Units providing or using electronic communications resources are similarly obligated to secure said resources when under their control, or to use electronic communications resources that meet campus and University standards.

See:

- *Appropriate Use Policy, Campus Administrative Manual, Article VIII, Section 1.1:* <http://www.cam.illinois.edu/viii/VIII-1.1.htm>
- *The Information Security Policy, Campus Administrative Manual, Article VIII, Section 1.2:* <http://www.cam.illinois.edu/viii/VIII-1.2.htm>
- Campus Information Technology Standards: <http://go.illinois.edu/itstandards>

15. Record Retention and Disposal

The General Rules of the University of Illinois at Article VI, Section 4b (see <http://www.uillinois.edu/trustees/rules.cfm#sec64>) provides that: "Records produced or

received by any agency or employee of the University in the transaction of University business become University property.”

Campus policy addressing the retention or destruction of University records can be found in the Campus Administrative Manual. Questions should be directed to the University Archivist.

- See: *Destruction or Transfer of University Records, Campus Administrative Manual, Article III, Section 6* at <http://www.cam.illinois.edu/iii/iii-6.htm>
- Electronic Records and Information Management, University Archives at <http://www.library.illinois.edu/archives/services/records.php>

16. Emergency Communications

In the interest of life safety or significant campus emergency, all University provided communications resources may be used to communicate information to the campus community, at the discretion of the Chancellor or the Head of the Division of Public Safety.

See: Campus Administrative Manual, Article V, Section A2 at <http://www.cam.illinois.edu/v/v-a-2.htm> for the campus emergency communications policy.

17. Email Addresses and other Identifiers for Electronic Communications

Email addresses and other electronic communications identifiers provided by the University or created to support the mission of the University are the property of the University of Illinois. Faculty and staff must conduct University business with each other and students through identifiers for whom the identity of the user can be verified as permitted by technology.

18. Contact Information

All systems, units and individuals are required to use the officially maintained contact information for official communications and notifications. This information is primarily sourced from the enterprise-wide information system (Sungard Banner) and made generally available through the Enterprise Data Warehouse and CITES directory services. Full compliance with this requirement will not be expected until July 1st, 2014 for situations where the necessary contact information exists and is available from the aforementioned primary sources. Units unable to comply with this by 7/1/2014 should request an exemption.

19. Faculty and Staff

19.1. Electronic communications commonly include both records of transitory value and records of long term value. Records of transitory value do not document a decision, policy, or process. Records of long-term value document a decision policy, or process; examples include but are not limited to: discussions related to human resources (hiring/firing/promotion/tenure), student and faculty interactions, financial assistance, purchases (p-card, procurement), athletic recruitment, etc. Any electronic communication, excluding phone conversations, containing records of long-term value must be transacted through a University provided account where an account can be provided.

19.2. All faculty and staff must use a campus or University provided official email service when conducting University business by email. Note: compliance with this provision will not be expected until approximately July 2012 when transition to a new campus wide email service will be completed. This policy will be updated with specifics at that time.

19.3. Faculty and staff may choose to use non-University provided or licensed communications and collaboration services as required by collaborators or professional communities in support of research and administration. However faculty should be aware that doing so may limit the University's ability to assist with security, copyright, or other intellectual

property disputes. Non-faculty staff should consult with their supervisor as to the appropriateness of using non-University provided electronic communication accounts or resources. Under no circumstance should units or individuals release any part of the student educational record without a contracted service relationship addressing the restrictions on use of student data as specified by FERPA. Contact the Office of the Registrar for guidance.

19.4. Faculty and staff may not forward their campus email alias or campus account to a third party email provider with whom the University does not contract for services.

19.5. Faculty and staff are expected to read their University provided email account on a regular basis in that this account will be used to provide individuals with timely and pertinent information related to their employment and the operation of the campus and University.

20. Educational use of Email and other forms of Electronic Communications

20.1. Faculty will determine how electronic forms of communication (e.g., websites, email, blogs, twitter, social networking, etc.) will be used in their classes and will specify their use and requirements in the course syllabus. Course syllabi will also contain the instructor's official University email address. Prior to posting any part of the student educational record to an online public forum, including course projects, enrollment or roster information, etc., faculty must get written consent from the individual student. Instructors must provide a way for students to "opt out" from public online posting.

20.2. Faculty and staff may share educational record information with individual students over a variety of electronic communications as long as the student first requests the information via an Illinois system that authenticates the student identity.

21. Students

21.1. Students are expected to read their University provided email account (or personal account if registered with the University), or other accounts as required by faculty as detailed in a course syllabus, on a regular basis. Any consequences arising from a failure to read any message sent to a student's account will be solely borne by the student.

21.2. Email notifications sent by the University (pertaining to, for example, financial aid, enrollment, and other academic related information) may only be sent to the University provided email alias. This requirement may be relaxed for new incoming students prior to their first day of instruction.

21.3. Email notifications sent by the University to the University provided email address will be assumed to have been successfully delivered to the student's email account.

21.4. Electronic communications sent to the University (including University officials, faculty, and staff) from students must come from a system where the identity of the student can be authenticated. Only such messages may be assumed to have been successfully delivered.

21.5. Students forwarding their email or registering a third-party account with the University are still obligated to read messages sent by University officials to the student email account.

22. Group, Departmental, or other Shared Accounts

Shared accounts are permitted when it is possible to create such accounts such that individual access to the account is through personally identifying credentials. For accounts supporting University activities the use of such shared accounts is strongly encouraged. Shared accounts should be treated as a unit resource, not used for any personal activity, and may be accessed as needed by the managing unit without special authorization. Individuals asked to manage shared accounts must be informed of the special status of shared accounts.

23. Exemption Requests

Requests for exemptions to this policy are made to the campus Chief Information Officer (CIO), who is assigned the responsibility for implementing this policy and ensuring that any exemptions granted are necessary and limited to support a legitimate University purpose. Exemption requests should be addressed to itpolicy@illinois.edu.

24. Definitions

24.1. University Official: "University officials" may include: (1) any person employed by the University in an administrative, supervisory, academic, research, student employee, or support staff position (including persons employed by the University law enforcement unit and health staff); (2) a person serving on an official committee, including but not limited to a scholarship, disciplinary or grievance committee, or otherwise assisting a University official in performing his or her tasks; (3) a person serving on the Board of Trustees; (4) a person or company with whom the University has contracted to provide a service (such as an attorney, auditor, or collection agent). See: *Student Code §3-602(e)*

24.2. Administrative Officer: As used in the section on Massmail, the administrative officer refers to the individual whose authority covers the entire group being messaged. For example, the Dean of Students for multi-unit student groups or the Provost's Office for multi-unit academic groups.

24.3. Official Communications: Any communications in any form that constitutes part of the operation of the University supporting its academic or research mission, public service and administrative functions in support of that mission.

24.4. Electronic Communications: The electronic transmission of information, as used in this policy to refer to email, text, chat, video, or similar means of electronically mediated human interaction.

24.5. Electronic Communications Resource: An account, program, or device used to support electronic communications.

24.6. Email Alias: An email alias is simply a forwarding address. For example, all campus email addresses of the form netid@illinois.edu are aliases for an actual email account such as netid@ad.illinois.edu. Use of an alias allows for replacement or changes to the email infrastructure (and thus the actual email address) without forcing a change to the publicly disseminated email address.

24.7. Shared Accounts: An electronic communications account used by two or more individuals.

24.8. Students: The term "students" as used in the scope statement includes admitted non-degree or degree seeking students who are eligible to enroll at the University.