V.I. POLICY ON PRIVACY IN THE ELECTRONIC ENVIRONMENT

(Source: University Council Resolution, April 26, 2000; Office of the Provost, Almanac, September 19, 2000 *(*https://almanac.upenn.edu/archive/v47/n04/OR-eprivacy.html*))*

I. Preliminary Observations

The University affirms that the mutual trust and freedom of thought and expression essential to the academic mission of a university rest on an expectation of privacy, and that the privacy of those who work, study, teach, and conduct research in a university setting will be respected. The University recognizes that as faculty, staff and students create, use and store more information in electronic form, there is growing concern that information the user or creator considers private may be more vulnerable to invasion than information stored in more traditional media. This policy is intended to highlight some general principles that should help to define the expectations of privacy of those in the University community. While no document addressing the fluid issue of technology can be exhaustive or inflexibly dictate outcomes in all circumstances, this policy attempts to articulate current practices and provide guidance, so that individuals may make informed and appropriate decisions concerning their various interactions in the electronic environment.

Before addressing these issues, it should also be noted that in carrying out their operations, various departments of the University accumulate information about members of its community, e.g., for purposes of payroll, employment or enrollment. Data are also created, though not necessarily compiled or retained on a personally identifiable basis, as an incident to the use of technology, e. g. , the charging of purchases on Penn Card or the borrowing of library books. The University does not condone disclosure or release of such personal information stored or transmitted through University systems, except for legitimate University purposes as outlined in this policy.

Those responsible for maintaining the University's computers and electronic networks have an important and special responsibility to recognize when they may be dealing with sensitive or private information. They may access such information without the user's consent and without obtaining higher level approval, but only when necessary to fulfill their official responsibilities, and they are expected to carry out their duties in ways that are not unreasonably intrusive. They will be subject to disciplinary action if they misuse their access to personally identifiable data or to individuals' personal files, e-mail and voice mail or otherwise knowingly act in ways counter to University policies and applicable laws.

Finally, this policy should be understood in light of the many other University policies and laws that bear on individuals' rights to privacy and the institution's responsibilities with respect to information in its possession about individuals.

Examples of applicable laws include the Family Educational Rights and Privacy Act of 1974 (the "Buckley Amendment"), the Electronic Communications Privacy Act of 1986, and medical records regulations promulgated under the Health Insurance Portability and Accountability Act of 1996. Examples of applicable University policies include the Acceptable Use Policy for the Electronic Environment, Administrative Computing Security Policy, Policy for Closed Circuit Television Monitoring and Recording of Public Areas for Safety and Security Purposes and policies on Records Confidentiality and Safeguarding University Assets.

II. Policy on Information Created, Stored or Transmitted Through University Electronic Media

A. In General:

The University provides computers, computer and e-mail accounts, networks and telephone systems to faculty members, staff and students for the purpose of furthering the University's academic mission and conducting University business. While incidental and occasional personal use of such systems, including e-mail and voice mail, is permissible, personal communications and files transmitted over or stored on University systems are not treated differently from business communications; there can be no guarantee that such personal communications will remain private or confidential (see Appendix at the end of this policy).

As is the case for information in non-electronic form stored in University facilities, the University's need for information will be met in most situations by simply asking the author or custodian for it. The University reserves the right, consistent with this policy, to access, review and release electronic information that is transmitted over or stored in University systems or facilities. When questions arise about such access, review or release of information, the University commits to treat electronic information no differently from non-electronic information. As with paper information, it is often the case by custom or rule that electronic files are shared and properly accessible by multiple parties in office settings. Where that is the case, the special provisions for access and notification outlined here need not be followed. In other cases, properly authorized University officials including the Vice President for Audit and Compliance and the Information Security Officer may access e-mail, voice mail or computer accounts without the consent of the assigned user when there is a reasonable basis to believe that such action

1. Is necessary to comply with legal requirements or process, or
2. May yield information necessary for the investigation of a suspected violation of law or regulations, or of a suspected serious infraction of University policy (for example alleged research misconduct, plagiarism or harassment), or
3. Is needed to maintain the integrity of University computing systems, or
4. May yield information needed to deal with an emergency, or
5. In the case of staff, will yield information that is needed for the ordinary business of the University to proceed.

Except as may otherwise be dictated by legal requirements, individuals will be notified of access to, or disclosure of, the contents of their e-mail, voice mail or their computer accounts as soon as practicable. In cases where such notification might jeopardize an ongoing investigation of suspected wrongdoing it may be delayed until the conclusion of the investigation. The Office of General Counsel is responsible for maintaining an official record of e-mail searches performed by authorized parties.

B. Faculty:

The University has the utmost respect for the freedom of thought and expression that are at the core of Penn's academic mission. Whenever possible, therefore, the University shall resolve any doubts about the need to access a University computer or other systems in favor of a faculty member's privacy interest. Computer files, e-mail

and voice mail created, stored, transmitted or received by faculty shall be afforded the same level of privacy as the contents of their offices. The Policy on Safeguarding University Assets governs access to faculty records in connection with investigations carried out by the University's Office of Audit and Compliance, and provides for prior consultation with the Provost and Faculty Senate and for notifying the subject of a search of any files or materials taken during an investigation. Except as may otherwise be dictated by legal requirements, the procedures outlined in that policy shall be followed with respect to a faculty member's computer files, e-mail or voice mail in connection with other investigations or proceedings.

C. Staff:
It is generally not University policy to access staff members' electronically stored information. As noted above, the University's need for information shall normally be met by asking an employee for it. Properly authorized University officials, including supervisors acting with the consent of their management, may, however, access, review and release the contents of staff computer files, e-mail or voice mail transmitted over or stored on University systems when, for example, an employee is absent or has left the University and the information is not available elsewhere, or in other situations in which it is necessary if the ordinary business of the University is to proceed. In more complicated situations - where, for example, a supervisor believes University resources are being misused - he/she should consult with senior administrators, the Division of Human Resources, or the Office of General Counsel.

D. Students:
Students are provided e-mail and computer accounts for use primarily in connection with their academic activities. While the University does not generally monitor or access the contents of a student's e-mail or computer accounts, it reserves the right to do so. However, access to and disclosure of a student's e-mail messages and the contents of his/her computer accounts may only be authorized by any one of the dean of the student's School or his/her designate, the Vice Provost for University Life, or the Office of Audit and Compliance, in consultation with the Office of General Counsel.

E. Multiple Affiliations:
Some individuals have multiple University affiliations (e. g. students employed by the University). When the need for access to information arises from a particular status, the provisions above for that status shall be applied. In other cases, the provisions for the individual's primary status shall be applied.

III. Violations of this Policy

Members of the University community who believe that this policy has been violated with respect to their privacy should attempt initially to resolve the issue within their unit or department, if necessary with the mediation of the leadership of their representative assembly or the University Ombudsman. Others who become aware of violations of this policy should report them to the University Information Security Officer, Office of General Counsel, Division of Human Resources or the Office of Audit and Compliance. All University offices that substantiate such violations should report them to the University Information Security Officer, who will monitor them for repeat instances and patterns. Those who violate this policy may be subject to disciplinary procedures up to and including dismissal.

Appendix: Special Note on E-mail Privacy

Despite the best intentions of users and the University or other system operators, it is difficult, if not impossible, to assure the privacy of e-mail. E-mail is not a good medium to use for sensitive matters that one would not want disclosed. There are numerous ways that plain text e-mail may be disclosed to persons other than the addressee, including:

- Recipient's address is mistyped; message is sent to someone else.
- Recipient forwards e-mail to someone else.
- Intruders break into e-mail system and read/disclose messages.
- Despite owner's belief that he/she deleted it, e-mail continues to exist on computer hard drive or a copy is archived on tape backup; disclosure of such copies may be required in connection with judicial or administrative proceedings or government investigations.
- E-mail is observed as it travels over public networks like PennNet and the Internet.
- In addition, e-mail users may want to consider routinely or periodically deleting old messages, and encrypting personal messages. Systems administrators should consider shorter retention of backup tapes, consistent with data integrity requirements.