

POLICY ON ACCEPTABLE USE OF ELECTRONIC RESOURCES

Summary

This policy defines the boundaries of “acceptable use” of limited University electronic resources, including computers, networks, electronic mail services and electronic information sources, as detailed below. It includes by reference a self-contained compilation of specific rules that can be modified as the electronic information environment evolves.

The policy is based on the principle that the electronic information environment is provided to support University business and its mission of education, research and service. Other uses are secondary. Uses that threaten the integrity of the system; the function of non-University equipment that can be accessed through the system; the privacy or actual or perceived safety of others; or that are otherwise illegal are forbidden.

By using University electronic information systems, you assume personal responsibility for their appropriate use and agree to comply with this policy and other applicable University policies, as well as City, State and Federal laws and regulations, as detailed below.

The policy defines penalties for infractions, up to and including loss of system access, employment termination or expulsion. In addition, some activities may lead to risk of legal liability, both civil and criminal.

Users of electronic information systems are urged in their own interest to review and understand the contents of this policy.

Purposes

The University of Pennsylvania makes computing resources (including, but not limited to, computer facilities and services, computers, networks, electronic mail, electronic information and data, and video and voice services) available to faculty, students, staff, registered guests, and the general public to support the educational, research and service missions of the University.

When demand for computing resources may exceed available capacity, priorities for their use will be established and enforced. Authorized faculty and staff may set and alter priorities for exclusively local computing/networking resources. The priorities for use of University-wide computing resources are:

Highest: Uses that directly support the educational, research and service missions of the University.

Medium: Other uses that indirectly benefit the education, research and service missions of the University, as well as and including reasonable and limited personal communications.

Lowest: Recreation, including game playing.

Forbidden: All activities in violation of the General Standards or prohibited in the *Specific Rules* interpreting this policy.

The University may enforce these priorities by restricting or limiting usages of lower priority in circumstances where their demand and limitations of capacity impact or threaten to impact usages of higher priority.

Implied consent

Each person with access to the University’s computing resources is responsible for their appropriate use and by their use agrees to comply with all applicable University, School, and departmental policies and regulations, and with applicable City, State and Federal laws and regulations, as well as with the acceptable use policies of affiliated networks and systems (See Appendices to *Specific Rules*).

Open Expression in the Electronic Information Environment: The rights to freedom of thought, inquiry and expression, as defined in the University’s Guidelines on Open Expression (<http://catalog.upenn.edu/pennbook/open-expression/>), are paramount values of the University community. The University’s commitment to the principles of open expression extends to and includes the electronic information environment, and interference in the exercise of those rights is a violation of this policy and of the Guidelines on Open Expression (<http://catalog.upenn.edu/pennbook/open-expression/>). As provided in the Guidelines (<http://catalog.upenn.edu/pennbook/open-expression/>), in case of conflict between the principles of the Guidelines on Open Expression (<http://catalog.upenn.edu/pennbook/open-expression/>) and this or other University policies, the principles of the Guidelines (<http://catalog.upenn.edu/pennbook/open-expression/>) take precedence.

General Standards for the Acceptable Use of Computer Resources: Failure to uphold the following General Standards for the Acceptable Use of Computer Resources constitutes a violation of this policy and may be subject to disciplinary action.

The General Standards for the Acceptable Use of Computer Resources require:

- Responsible behavior with respect to the electronic information environment at all times;
- Behavior consistent with the mission of the University and with authorized activities of the University or members of the University community;
- Respect for the principles of open expression;
- Compliance with all applicable laws, regulations, and University policies;
- Truthfulness and honesty in personal and computer identification;
- Respect for the rights and property of others, including intellectual property rights;
- Behavior consistent with the privacy and integrity of electronic networks, electronic data and information, and electronic infrastructure and systems; and
- Respect for the value and intended use of human and electronic resources.

Enforcement and Penalties for Violation: Any person who violates any provision of this policy, of the *Specific Rules* interpreting this policy, of other relevant University policies, or of applicable City, State, or Federal laws or regulations may face sanctions up to and including termination or expulsion. Depending on the nature and severity of the offense, violations can be subject to disciplinary action through the Student Disciplinary System or disciplinary procedures applicable to faculty and staff.

It may at times be necessary for authorized systems administrators to suspend someone’s access to University computing resources immediately for violations of this policy, pending interim resolution of the situation (for example by securing a possibly compromised account and/or making the owner of an account aware in person that an

activity constitutes a violation). In the case of egregious and continuing violations suspension of access may be extended until final resolution by the appropriate disciplinary body.

System owners, administrators or managers may be required to investigate violations of this policy and to ensure compliance.

Amendment

Formal amendment of the General Standards of Acceptable Use of Computing Resources or other aspects of this policy may be promulgated by the Provost following consultation with the University Council Committee on Communications, publication "For Comment" in *Almanac*, a reasonable waiting period, and publication "Of Record" in *Almanac*.

Interpreting this Policy

As technology evolves, questions will arise about how to interpret the general standards expressed in this policy. The Vice President for Information Systems and Computing shall, after consultation with the University Council Committee on Communications, and subject to the same waiting period and publication provisions as above, publish specific rules interpreting this policy.

Waiver

When restrictions in this policy interfere with the research, educational or service missions of the University, members of the University community may request a written waiver from the Vice President for Information Systems and Computing (<http://www.upenn.edu/computing/isc/>) (or designee).

Further Information

For further information about University computing regulations or Commonwealth of Pennsylvania and Federal computing laws, contact the University Information Security Officer at (215) 898-2172 or send email to: security@isc.upenn.edu.

Specific Rules Interpreting the Policy on Acceptable Use of Electronic Resources

The following specific rules apply to all uses of University computing resources. These rules are not an exhaustive list of proscribed behaviors, but are intended to implement and illustrate the General Standards for the Acceptable Use of Computer Resources, other relevant University policies, and applicable laws and regulations. Additional specific rules may be promulgated for the acceptable use of individual computer systems or networks by individual Schools, departments, or system administrators.

Content of Communications

- Except as provided by applicable City, State, or Federal laws, regulations or other University policies, the content of electronic communications is not by itself a basis for disciplinary action.
- Unlawful communications, including threats of violence, obscenity, child pornography, and harassing communications (as defined by law), are prohibited.
- The use of University computer resources for private business or commercial activities (except where such activities are otherwise permitted or authorized under applicable University policies), fundraising or advertising on behalf of non-University organizations, or the reselling of University computer resources to non-University

individuals or organizations, and the unauthorized use of the University's name, are prohibited. The Vice President for Information Systems (or designee) may specify rules and specific forums where limited use of University resources for non-recurring exchange and sale of personal items is permitted.

Identification of Users

Anonymous and pseudonymous communications are permitted except when expressly prohibited by the operating guidelines or stated purposes of the electronic services to, from, or through which the communications are sent. However, when investigating alleged violations of the Guidelines on Open Expression (<http://catalog.upenn.edu/pennbook/open-expression/>), the Committee on Open Expression may direct the University's Information Security Officer, or an authorized system administrator, to attempt to identify the originator of anonymous/pseudonymous messages, and may refer such matters to appropriate disciplinary bodies to prevent further distribution of messages from the same source.

The following activities and behaviors are prohibited:

- Misrepresentation (including forgery) of the sender's identity or an electronic communication's source;
- Acquiring or attempting to acquire passwords of others;
- Using or attempting to use the computer accounts of others;
- Alteration of the content of a message originating from another person or computer with intent to deceive; and
- The unauthorized deletion of another person's news group postings.

Access to Computer Resources

The following activities and behaviors are prohibited:

- The use of restricted-access University computer resources or electronic information without or beyond one's level of authorization;
- The interception or attempted interception of communications by parties not explicitly intended to receive them;
- Making University computing resources available to individuals not affiliated with the University of Pennsylvania without approval of an authorized University official;
- Making available any materials the possession or distribution of which is illegal;
- The unauthorized copying or use of licensed computer software;
- Unauthorized access, possession, or distribution, by electronic or any other means, of electronic information or data that is confidential under the University's policies regarding privacy or the confidentiality of student, administrative, personnel, archival, or other records, or as defined by the cognizant Data Steward;
- Intentionally compromising the privacy or security of electronic information; and
- Intentionally infringing upon the intellectual property rights of others in computer programs or electronic information (including plagiarism and unauthorized use or reproduction).

Operational integrity

The following activities and behaviors are prohibited:

- Interference with or disruption of the computer or network accounts, services, or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses", the sending of

- electronic chain mail, and the inappropriate sending of “broadcast” messages to large numbers of individuals or hosts;
- Failure to comply with requests from appropriate University officials to discontinue activities that threaten the operation or integrity of computers, systems or networks, or otherwise violate this policy;
- Revealing passwords or otherwise permitting the use by others (by intent or negligence) of personal accounts for computer and network access;
- Altering or attempting to alter files or systems without authorization;
- Unauthorized scanning of networks for security vulnerabilities;
- Attempting to alter any University computing or networking components (including, but not limited to, bridges, routers, and hubs) without authorization or beyond one’s level of authorization;
- Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or re-transmission of any computer or network services;
- Intentionally damaging or destroying the integrity of electronic information;
- Intentionally disrupting the use of electronic networks or information systems;
- Intentionally wasting human or electronic resources; and
- Negligence leading to the damage of University electronic information, computing/networking equipment and resources.

- Protocols for human subjects research: any research involving human subjects must be approved by the Committee on Studies Involving Human Beings
- Acceptable Use Policies of individual Schools, departments, computer systems, and networks
- Guidelines for Administrators of Penn E-mail Systems (<https://provider.www.upenn.edu/computing/email/admin-guidelines.html>)

Applicable laws

Computer and network use is also subject to Pennsylvania and Federal laws and regulations. Suspected violations of applicable law are subject to investigation by University and law enforcement officials. Among the applicable laws are:

- *Federal Copyright Law*: U.S. copyright law grants authors certain exclusive rights of reproduction, adaptation, distribution, performance, display, attribution and integrity to their creations, including works of literature, photographs, music, software, film and video. Violations of copyright laws include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recordings) and distributing copyrighted materials over computer networks or through other means.
- *Federal Wire Fraud Law*: Federal law prohibits the use of interstate communications systems (phone, wire, radio, or television transmissions) to further an illegal scheme or to defraud.
- *Federal Computer Fraud and Abuse Law*: Federal law prohibits unauthorized access to, or modification of information in computers containing national defense, banking, or financial information.
- *Federal and Pennsylvania Child Pornography Laws*: Federal and Pennsylvania laws prohibit the creation, possession, or distribution of graphic depictions of minors engaged in sexual activity, including computer graphics. Computers storing such information can be seized as evidence.
- *Pennsylvania Computer Crime Law*: Pennsylvania law prohibits access to any computer system or network with the intent to interrupt an organization, or to perpetrate a fraud including the intentional and unauthorized publication of computer passwords.
- *Pyramid Schemes/Chain Letters*: It is a violation of the Federal Postal Lottery Statute to send chain letters which request sending money or something of value through the US mail. Solicitations through electronic messaging are also illegal, if they require use of US mail for sending money/something of value.
- *Defamation*: Someone may seek civil remedies if they can show that they were clearly identified as the subject of defamatory messages and suffered damages as a consequence. Truth is a defense against charges of defamation.
- *Common law actions for invasion of privacy*: Someone may take seek civil remedies for invasion of privacy on several grounds.
- *Public disclosure of private facts*: the widespread disclosure of facts about a person, even when true, may be deemed harmful enough to justify a lawsuit.
- *False light*: a person wrongfully attributes views or characteristics to another person in ways that damage that person’s reputation.
- *Wrongful intrusion*: the law often protects those areas of a person’s life in which they can reasonably expect they will not be intruded upon.

(Source: Almanac, April 29, 1997 (<http://www.upenn.edu/almanac/v43/n32/accept.html>))

Appendices

Relevant University policies

This Acceptable Use Policy incorporates and supersedes the earlier Policy on Ethical Behavior with Respect to the Electronic Information Environment. The use of computing resources is also required to conform to the following University policies:

- Code of Student Conduct (<http://catalog.upenn.edu/pennbook/code-of-student-conduct/>)
- Guidelines on Open Expression (<http://catalog.upenn.edu/pennbook/open-expression/>)

In addition, specific policies of the University’s Schools, departments, computer systems and networks, and other general University policies and regulations are also applicable to the use of computer resources. These policies include, but are not limited to, the following:

- Patent Policy (<http://catalog.upenn.edu/pennbook/patent-tangible-research-property-policies-procedures/>)
- Copyright Policy (<http://catalog.upenn.edu/faculty-handbook/v/v-1/>)
- Computer Software Policy (<http://www.upenn.edu/almanac/v45/n08/copy.html>)
- Policy on the Uses of University Resources (<https://www.hr.upenn.edu/policies-and-procedures/policy-manual/other-policies/uses-of-university-resources/>)
- Policy on Confidentiality of Student Records and Information (<http://catalog.upenn.edu/pennbook/confidentiality-student-records/>)
- Policy Regarding Faculty Misconduct in Research (<http://catalog.upenn.edu/faculty-handbook/iii/iii-b/>)
- Policy on Privacy in the Electronic Environment (<http://catalog.upenn.edu/pennbook/policy-privacy-electronic-environment/>)
- Code of Academic Integrity (<http://catalog.upenn.edu/pennbook/code-of-academic-integrity/>)