

THE UNIVERSITY OF IOWA



October 12, 1998

President, Faculty Senate
President, Staff Council
President, UISG
Chair, UIHC Hospital Advisory Committee

Dear Colleagues:

Enclosed for review please find the most recent draft of a revised Acceptable Use of Information Technology Resources policy that has been generated by an *ad hoc* committee over the past year. (Current policy may be found in the *University Operations Manual II-19*.) While we have had input from many sources to date, we would now like to have whatever formal review each constituent organization feels appropriate. If this target is consistent with the practices of your organization, we would hope we might get feedback before the end of fall semester.

In what follows, I will attempt to give you some additional background. However, let me indicate that I and other members of the committee would be happy to attend any appropriate meeting to answer additional questions or get feedback more directly.

Over the past several years, it had come to the attention of several of us that our existing acceptable use policy left unanswered some very practical questions. We also became concerned that unless the University developed a rather comprehensive policy, one might be imposed on us from outside the University.

The members of the *ad hoc* committee who participated in drafting or reviewing this proposed policy included the following: Sue Buckley, Stephana Colbert, Barbara Dewey, Bob Foldesi, Shelly Kurtz, Susan Mask, Chris Pruess, Mark Schantz, and Mary Jo Small.

The committee reviewed some policies from peer institutions and borrowed some of the key security and privacy portions of the new policy draft of Ohio State University, a policy undergoing a similar campus review as this one. What we hope we have achieved is identification of some of the best practices and tailoring of them to the particular situation here at the University of Iowa.

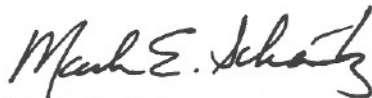
In preparing the draft policy, we attempted to balance appropriately a number of concerns and objectives. There are a number of misconceptions about the electronic environment that we hoped to dispel. On the one hand, many people wrongly believe that the legal principles applicable to print and telephonic media are somehow inapplicable to e-mail and the Internet. On the other hand, many others are under the erroneous impression that e-mail and other computer files are as secure as first-class mail. In reviewing the draft policy, you will observe that we stress the desire to provide an environment which will foster free interchange of ideas and recognize that privacy is often important to that end. However, we also try to make clear the significant number of occasions upon which complete privacy may not be available.

We also attempted to find the right balance between protecting the University from liability and protecting the rights of users of our resources. We do not wish to become a "publisher" as that term is used in the law of defamation. In other words, we do not wish to be obliged to screen the many myriad communications that utilize our resources and to be responsible for before-the-fact prevention of every misuse of the technology. Rather, we wish to limit our exposure to those situations where we have knowledge of a problem in advance via a complaint.

We also felt it necessary to address the issue of personal use. The policy sets forth the general principle that faculty and staff may use University IT facilities only for University-related educational and administrative purposes. The policy goes on to describe how this principle should be applied by providing a section entitled, "Individual Responsibilities." For example, Section IV.F contrasts the kinds of modest personal use which may be considered to contribute to the University's mission with uses which are excessive and impermissible. To provide further guidance to faculty and staff, the policy also charges individual departments to develop policies defining what constitutes the work of the unit for which use of IT resources is acceptable.

After you have had an opportunity to analyze the policy, we would very much like to hear from you as to any concerns that you may have or suggestions for improvement. You will be able to access and review an on-line copy of this policy draft at <http://www.uiowa.edu/homepage/policy/draft/>. You may submit comments electronically to itaup@list.uiowa.edu. Thanks in advance for your assistance.

Very truly yours,



Mark E. Schantz
General Counsel

Enclosure

Acceptable Use of Information Technology Resources Policy

D R A F T

I. PREAMBLE

The University of Iowa's Information Technology Resources have been assembled to facilitate the pursuit of excellence in the University's missions of teaching, research and service. The opportunity to use computing systems and software, as well as internal and external data networks, is important to all members of the University community. To preserve that opportunity for the full community, each individual faculty member, staff member and student must comply with institutional and external standards for acceptable use. Except as otherwise provided in this policy, University-supplied computers, software, and other computer-related technologies should be used only for University-related educational and administrative purposes. By using University information technology facilities and resources, users agree to abide by all related University policies and procedures, as well as applicable federal, state and local law. Violations may result in University disciplinary action or referral to appropriate external authorities.

The use of University computing resources—like the use of any other University provided resource and like any other university-related activity—is subject to the normal requirements of legal and ethical behavior within the University community. Thus, legitimate use of a computer, computer system, switching system, or network does not extend to whatever is technically possible. Although some limitations are built into computer operating systems and networks, those limitations are not the sole restrictions on what is permissible. Users must abide by all applicable restrictions, whether or not those restrictions are built into the operating system or network and whether or not they can be circumvented by technical means.

II. SCOPE OF POLICY

This acceptable use policy applies to all users of University information technology resources under the management or control of Information Technology Services (ITS) or other units of the University of Iowa such as UIHC Hospital Information Systems (HIS). A "user" is defined as any individual who uses, logs in to, or attempts to use or log in to, a system; or who connects to, or attempts to connect to or traverse a network, whether by hardware or software or both, whether on campus or from remote locations. The term "user" thus includes system sponsors and system managers, faculty, staff, students, and other customers. "Information technology resources" are those facilities, technologies and information resources required to accomplish information processing, storage and communication, whether individually controlled or shared, stand-alone or networked. Included in this definition are all Information Technology Centers (ITC), classroom technologies, electronic resources, and computing and electronic communication devices and services, such as, but not limited to, computers, printers, modems, e-mail, phone,

voice-mail, fax transmissions, video, ISIS, OASIS, multi-media, instructional materials, and healthcare and administrative systems.

III. SECURITY AND PRIVACY

The same principles of academic freedom and privacy that have long been applicable to written and spoken communications in the University community apply also to electronic information. The University cherishes the diversity of perspectives represented on this campus and, accordingly, does not condone either censorship or the casual inspection of electronic files.

The University employs various measures to protect the security of its computing resources and of their users' accounts. Users should be aware, however, that the University cannot guarantee such security. Users should therefore engage in "safe computing" practices by establishing appropriate access restrictions for their accounts, guarding their passwords, and changing passwords regularly. Users are responsible for maintaining backup and recovery systems in accordance with disaster recovery guidelines, as well as for implementing and maintaining computer security in accordance with best practices and University policies and procedures. The University respects encryption rights on its networks and may itself encrypt information and transactions when secure confidentiality is an obligation. In order to protect the security of the network, the department is responsible for ensuring that any personally-owned equipment connected to the network is being used for University purposes.

Users should also be aware that their uses of University computing resources are not completely private. While the University does not routinely monitor individual usage of its computing resources, the normal operation and maintenance of the University's computing resources require the backup of data and communications, the logging of activity, the monitoring of general usage patterns, and other such activities that are necessary for the rendition of service. The University may also specifically monitor the activity and accounts of individual users of University computing resources, including individual login sessions and communications, without notice, when (a) the user has voluntarily made them accessible to the public, as by posting to Usenet or a web page; (b) it reasonably appears necessary to do so to protect the integrity, security, or functionality of University or other computing resources or to protect the University from liability; (c) there is reasonable cause to believe that the user has violated, or is violating, this policy; (d) a user appears to be engaged in unusual or excessive activity, as indicated by the monitoring of general activity and usage patterns; (e) a supervisor or principal investigator finds it necessary to retrieve a file of assigned work; or, (f) monitoring is otherwise required by law. Any such individual monitoring, other than that specified in (a), (e), or (f), or necessary to respond to emergency situations, must be authorized in advance by the Director of ITS or by the Director's designee, or for UIHC, the Director of HIS, in consultation with University Counsel. The University, in its discretion, may disclose the results of any such general or individual monitoring, including the contents and records of

individual communications, to appropriate University personnel or law enforcement agencies and may use those results in appropriate University disciplinary proceedings.

In addition, users should be aware that their right to privacy in electronic records may be subject to the University's obligation to respond to *subpoenas* or other court orders, reasonable discovery requests, and requests for documents pursuant to Iowa Code Chapter 22, the Public (Open) Records Law. University administrative records are subject to public record requests, unless an express exception recognizes the confidentiality of the material, such as the exception for library records. By statute, public records include all "records, documents, tape or other information, stored or preserved in any medium," whether generated by University administrators, faculty, or staff. The statute contains no express exception for documents generated by faculty or staff in the course of their employment. Although it is the University's position that personal electronic files of faculty, staff, and students are not ordinarily to be considered "public records," users should be aware that a court of law, and not University officials, may ultimately decide such issues.

IV. INDIVIDUAL RESPONSIBILITIES

A. Use resources appropriately. Uses that interfere with the proper functioning of the University's information technology resources are prohibited. Such inappropriate uses would include but are not limited to insertions of viruses into computer systems, tapping a network or running a "sniffer" program, e-mail spam, chain letters, destruction of another's files, use of software tools that attack IT resources, violation of security standards, and the like.

B. Respect the rights of others. Interference with the ability of other users to make appropriate use of the resources is prohibited. Such inappropriate uses include, without limitation, invading the privacy of another's files or otherwise gaining unauthorized access to the files of another. Such uses would include but are not limited to denial of service attacks, misrepresentation, forgery, use of software tools that attack IT resources, and the like.

C. Adhere to the EDUCAUSE Code of Software and Intellectual Rights. The EDUCAUSE Code follows:

Respect for intellectual labor and creativity is vital to academic discourse and enterprise. This principle applies to works of all authors and publishers in all media. It encompasses respect for the right to acknowledgment, right to privacy, and right to determine the form, manner, and terms of publication and distribution.

Because electronic information is volatile and easily reproduced, respect for the work and personal expression of others is especially critical in computer environments. Violations of authorial integrity, including plagiarism, invasion of privacy, unauthorized access, and trade secret and copyright violations, may be grounds for sanctions against members of the academic community.

D. Adhere to data access policies. Accessing restricted data or data not required for performance of an employee's job without authorization or permission is prohibited. Where access to restricted data is permitted, use of such data shall be limited to the purpose for which access was authorized. Secondary use of university data subject to access restriction, without adhering to the restrictions, is also not permitted.

Patient medical information retained by the University of Iowa Hospitals and Clinics is further protected by State law which prohibits any disclosure without specific written consent of the person to whom it pertains, or as otherwise required by law. A general authorization for release of medical or other information is not sufficient for this purpose.

E. Adhere to software licenses. Persons loading software on any University computer must adhere to all licensing requirements for the software. Except where allowed by University site licenses, copying software licensed for University use for personal use is a violation of this policy. Users are responsible for adhering to agreements for databases licensed by the University. Individual departments are charged with the responsibility of ensuring that licensing requirements are met and for developing a statement guiding the installation of personal software on departmental computers.

F. Avoid excessive personal use. Although modest personal use may improve the skills of individual users and otherwise contribute indirectly to the University's mission, excessive personal use can infringe upon the rights of others. Personal use may be excessive if it takes place during regularly scheduled work time, if it overburdens a network, if it results in substantial use of system capacity, or if it otherwise subjects the institution to increased operating costs. Some uses will be plainly excessive in all environments, but the extent to which other uses become excessive may vary among units. In those instances, supervisors will provide more specific guidance to individual users by formulating unit policies or providing advice on a case-by-case basis.

G. Refrain from prohibited personal uses. Information technology resources shall not be used for commercial activities or otherwise for personal gain, for unauthorized charitable solicitation, or for personal political activities such as campaigning for candidates for public office or unauthorized lobbying of public officials. Faculty and staff consulting that is in conformity with University guidelines is not a prohibited personal use. Use of the University's electronic address (e-mail, web) for the personal uses described above is prohibited.

H. Use University name as authorized. Unless authorized to speak for the University, users should avoid creating the impression they are doing so. Electronic exchange of ideas is encouraged. However, users shall take appropriate steps to avoid the possible inference that communication of a message via the University e-mail system or posting to an electronic forum connotes official University authorization or endorsement of the message.

Web pages and web links present on official University pages must be consistent with the work of the sponsoring unit. Links to commercial or for-profit entities may be appropriate as part of the work of the unit. However, advertisements, including logos, for commercial and other for-profit entities are not allowed, as they may be construed as a prohibited University product endorsement.

I. Adhere to other University policies. Inappropriate use of electronic technology resources may violate a number of generally applicable University policies, including, without limitation, University *Operations Manual* Sections III-15 Ethics and Academic Responsibility, V-24 Telephone Procedures, V-31 Intellectual Property, II-3 Human Rights, II-4 Sexual Harassment and II-10 Violence, IV-9 Fund Solicitation Policy, and Section IIA of "Policies and Regulations Affecting Students," and "Regents Guidelines on Union Organizing Activity."

J. Obey external laws. Information technology resources shall not be used in a manner that violates federal, state, or local law, including without limitation the federal requirement that the University provide employment and educational environments free from race-based or gender-based hostility (see Titles VI and VII, Civil Rights Act of 1964, and Title IX, Educational Amendments of 1972); and, state criminal laws forbidding harassment (Iowa Code Section 708.7), exhibition of obscene materials to minors (Iowa Code Section 728.2), rental or sale of hard core pornography (Iowa Code Section 728.4), official misconduct (Iowa Code Chapter 721), offenses against the government (Iowa Code Chapter 718), computer crime (Iowa Code Chapter 716A), and federal and state copyright and fair use laws. Nothing in this policy prohibits the use of appropriate material for educational purposes in any accredited school, or any public library, or in any educational program in which the minor is participating. Nothing in this policy prohibits the presence of minors at an exhibition or display of the use of any materials in any public library.

V. ADMINISTRATION AND ENFORCEMENT

Information Technology Services is charged with communicating this policy to the user community and for providing educational programs to achieve technical proficiency and appropriate use of the resources. Requests for interpretation of the policy as applied to particular situations may be directed to the appropriate University administrator, such as the Office of the Provost, Student Services, Human Resources, Affirmative Action, HIS, ITS or to the Office of the General Counsel.

Reports of apparent violations of the policy may be made to Information Technology Services, to an employee's supervisor or, in the case of a student, to the Office of the Vice President for Student Services. Where violations of law are alleged, University Public Safety or the Office of the General Counsel should be contacted. Appropriate sanctions will be imposed for violations of this policy by users. Sanctions may include an informal or formal reprimand, loss of user privileges for a definite or indefinite period, termination of employment, or, in the case of a student, probation, suspension, or expulsion from the

University.

Violation of this policy by faculty members will be treated as an ethics violation and governed by the general Faculty Dispute Procedures. (See Sections III-29 *et seq.* of the *University Operations Manual*.) Violations of this policy by staff members will be addressed by the staff member's supervisor, departmental executive officer, dean, Provost, or vice president. Appeals from any formal disciplinary action taken against a professional and scientific staff member are governed by the Policy Establishing Grievance Procedures for Professional and Scientific Personnel, Section III-28.4 of the *University Operations Manual*. Organized Merit staff have access to a contractual grievance procedure, and non-organized Merit staff have a procedure available under the Regents Merit System Rules. Violations of this policy by students will be governed by the Judicial Procedure for Alleged Violations of The Code of Student Life. Both the Code of Student Life and the Judicial Procedure are published and distributed to students annually in "Policies and Regulations Affecting Students."

VI. DISCLAIMER

The University makes no warranties of any kind, whether expressed or implied, with respect to the information technology services it provides. The University will not be responsible for damages resulting from the use of communication facilities and services, including, but not limited to, loss of data resulting from delays, non-deliveries, missed deliveries, service interruptions caused by the negligence of a University employee, or by the user's error or omissions. Use of any information obtained via the Internet is at the user's risk. The University specifically denies any responsibility for the accuracy or quality of information obtained through its electronic communication facilities and services, except material represented as an official University record. The University also does not accept responsibility for removing material that some users may consider defamatory or otherwise offensive. Users should be advised, however, that dissemination of such material may subject them to liability in other forums.

VII. OTHER POLICIES AND RULES

Individual units within the University may define by written policies conditions of use for facilities under their control. Policy statements must be consistent in principle with this University policy, but may provide additional detail, guidelines or restrictions. Such unit or departmental policies should be submitted to the Provost (for faculty), Human Resources or Vice Presidents of the University (for staff), or to the Hospital Advisory Committee (for UIHC) to review for consistency with University policy. In addition, users are advised that network traffic exiting the University is subject to the acceptable use policies of our national and international network connectivity providers (e.g., ICN, vBNS, Internet2, or long distance communication providers such as MCI or AT & T).