

UMKC Policy on Privacy in the Use of University Communication Systems

The University of Missouri-Kansas City affirms that fulfilling the academic mission of a university requires unfettered freedom of thought and expression. The University is a community dedicated to the life of the mind and to the free and open exchange of ideas. The teaching, research, service, learning, and support activities conducted by faculty members, administrators, students, and staff members require the use of communications systems of various sorts, which are owned and maintained by the University of Missouri. We recognize that the free exchange of ideas and opinions, as well as many aspects of the teaching, research, and support work conducted on campus, are not possible without the explicit and implicit expectation of privacy and confidentiality in the communications of faculty, administrators, staff, and students. Thus, in all of our policies and practices, we recognize the individual's right to privacy to the fullest extent possible under all applicable laws.

At the same time, the University community realizes that, as faculty, administrators, staff, and students create, store, and use more and more information in electronic form and in more traditional media, serious concerns over the possible invasion of privacy and unauthorized sharing of information increase. The University also recognizes that, in the course of maintaining the communication systems, incidental access to private, confidential, and copyrighted information is sometimes unavoidable. Moreover, in performing their assigned duties, various departments or units of the University need to gather information about members of the university community for purposes of employment, payroll, enrollment, and so on. Thus, this policy on privacy is designed to enable authorized employees to perform their duties, subject to the limitations stipulated below and in associated policies. The University also recognizes that authorized Information Technology (IT) employees must be enabled to take, in a timely fashion, the actions necessary to protect the integrity of the University's communication systems and to comply with local, state, and federal laws. Whenever possible, authorized users will be notified before their computer files are accessed by authorized individuals.

The policy below, while not exhaustive, is intended to establish basic principles that will serve to delineate the expectations of privacy by authorized users of the University's communication systems. It also is intended to protect the rights of all authorized users and the University, as more detailed policies and practices are established. At the same time, this policy is designed to protect IT and other employees from any pressure from any quarter to invade the privacy of authorized users and to share or provide private, confidential, or copyrighted information with others. Employees will be able to refuse requests for such information by referring the request to the Oversight Committee, as described below, for its consideration and approval or refusal.

Those employees hired to maintain, protect, and upgrade the University's computing and electronic networks also have an important responsibility to understand the University's privacy policy and to conduct their work accordingly. In the course of their day-to-day operations, designated IT employees may have access to sensitive, private, copyrighted, and confidential information held by authorized users of the University's communication systems. Except when such incidental access is unavoidable in the process of maintaining the integrity of the communication systems, access to such information is explicitly prohibited. Even in such cases where incidental contact is unavoidable, the implicit and explicit expectations of privacy on the part of authorized users shall not be violated. That is, the private and confidential nature of the

information and communications shall be strictly preserved. Any individual who knowingly violates the privacy of others and/or the University policy on privacy is subject to disciplinary, administrative, and legal action.

Special Note on Email Privacy

Despite the best intentions of authorized users, the University, and other system operators, it is impossible to assure the absolute privacy of e-mail and other forms of electronic communication. There are numerous ways that plain text e-mail may be disclosed to persons other than the intended addressee, including: the recipient's address is mistyped; the recipient forwards your e-mail to someone else; unauthorized individuals break into the communications system and gain access to emails; you mistakenly hit the "reply to all" button, when you intend to communicate with only one or several persons on the list; you leave your computer on when it is accessible to others walking by. As a general rule, e-mail is not a good medium to use for sensitive matters that you do not want disclosed. In addition, the Sunshine Law in Missouri, as interpreted by the courts up to this time, potentially subjects all e-mail communications on the University system to disclosure to reporters and others who seek access to such communications. Finally, all users should be aware that, as e-mail travels over the Internet, it is observed by various non-university agencies.

1. Governing Principles

- The University recognizes that all authorized users of university computer networks, equipment or connecting resources have a right of privacy in such use.
- Privacy, confidentiality, and the values of freedom of thought and expression so essential to the integrity of the academic institution shall be paramount.
- The University will maintain a functional computer network system available to all authorized users and will protect and respect privacy of all authorized users.

2. Authorized Users: Faculty, staff, students and authorized guest users.

3. Inspection and Disclosure

- A. The University acknowledges and honors the governing principles set forth in paragraph 1 above but reserves the right, within the guidelines set by the oversight committee described below, to examine the information on its networks and equipment when:
- a. there are reasonable grounds to believe that a user is abusing the electronic system as abuse is defined below;
 - b. it is necessary in order to repair, maintain or improve the computer networks;
 - c. it is necessary to prevent legally recognized injury to another person, property or system; and
 - d. rules of duly enacted law or judicial decision require inspection.

- B. The oversight committee described below will develop and publish guidelines, which will:
- a. provide specifically limited authorization to identified persons within the University to examine and inspect its networks and equipment, and to make only those disclosures that are required (see Notice 3.C).
 - b. establish acceptable procedures for inspection of networks and equipment for known conditions and for required disclosures, including such steps as isolating or shutting down network components or equipment, preserving evidence of abuse, informing the suspected abuser of these actions, as soon as possible, and defining allowable remote and direct procedures for inspection and threat assessment, which preserve privacy and confidentiality to the maximal extent achievable. No interception, examination, monitoring, recording, copying or disclosure of computer produced materials by authorized users of the network shall occur except with reasonable suspicion of abuse and as explicitly allowed by these procedures. Administrative action, authorized by the oversight committee, will be taken against any person who violates the privacy, confidentiality and free speech rights of authorized users.
 - c. establish guidelines and procedures for unforeseen circumstances with the intent to protect and preserve the governing principles of privacy and confidentiality, and to protect the legitimate interests of the University to control and maintain the integrity and use of the network resources. These guidelines will define allowable limited appropriate action by authorized personnel. They will include procedures to assess the specific situation encountered and timely consultation with the oversight committee to evaluate the actions taken by Information Systems' staff, to approve further action(s) deemed necessary, and, when needed, to develop acceptable procedures for future responses.
- C. Notice: In all cases where the privacy of the user will be compromised as authorized above, notice of such intrusion will be given to the user in advance of the intrusion unless such notice will clearly prejudice the ability of the University to further its interests.

4. Abuse

Abuse of the network or any part thereof shall consist of the following:

- Violation of the Acceptable Use Policy (University of Missouri, Collected Rules and Regulations 110.005);
- Violation of Federal or State Law in a manner making it more likely than not that the University will incur legal liability;
- Violation of the expectations of privacy, confidentiality or free speech of an authorized user.

5. Oversight

A. The oversight committee will consist of:

- a. three faculty representatives: one member elected from among Faculty Senators and two members at large, elected from among the UMKC faculty by Faculty Senate election processes;
- b. two student representatives selected and appointed by the Student Government Association in such a way that one member is an undergraduate student and one member is a graduate student;
- c. two staff representatives at large, elected from among the UMKC staff by a Staff Council election process;
- d. one administration representative, appointed by the Chancellor;
- e. a representative from Libraries as an ex-officio, non-voting member;
- f. the Executive Director of Information Services or his designate as an ex officio, non-voting member;
- g. the Chief Information Officer as an ex officio, non-voting member.

B. Each member is elected or appointed for a 2-year term in such a way that maximal staggering of terms of membership for each represented group is achieved.

C. The committee will elect its own chair.

D. The committee will meet at least once per regular semester.

E. Any two members can convene the committee.