ACCEPTABLE USE POLICY (AUP)
FOR MSU INFORMATION TECHNOLOGY RESOURCES

Frequently Asked Questions (FAQ)

27 September 2011

1. Why is the AUP being revised?

   The current AUP was last revised in the summer of 1992. The “Internet”, as we know it today, was still an emerging technology with relatively few points of connection. For example, Mosaic (the first widely used browser for the emerging “World Wide Web”) was introduced in 1993, Microsoft’s Internet Explorer launched in 1995, and the graduate research project which resulted in the formation of Google began in March 1996.

   At the time the original AUP was drafted, the University was one of the very few channels in Michigan through which anyone could connect to the Internet to do online messaging (what became “e-mail”), data and document sharing, or what became “Web publishing.” In the almost 20 years since the AUP’s last revision, the Internet environment itself, and the laws, commercial services, and social expectations related to Internet usage, have changed greatly; the AUP must respond to these changes.

2. What are “local” rules and how might they differ from the AUP?

   “Local” rules may apply to specific systems or services, or to particular environments or offices. For example: use of systems or services that involve MSU Confidential Data types, as defined by the Institutional Data Policy, may be restricted to certain business purposes; systems used for payment card processing may be restricted only to that specific purpose; offices where employees and their workspace are highly visible to the public may prohibit use of office workstations to play games or to engage in personal shopping or other non-business activities.

3. Why can’t I use the MSU IT resources to do whatever I want? Don’t I have a First Amendment right to do so?

   The University’s IT resources are not a public forum. The resources are provided for University-related purposes. Although the University permits a de minimus amount of personal use as a matter of convenience to members of the University community, the primary purpose of the resources is to support the University’s teaching, research, and public service missions, its administrative functions, and student and campus life activities. Other avenues and resources outside the University exist for members of the University community to conduct their personal business and express their personal views.
4. **What does Section 2.3.1 mean when it states that personal use is prohibited if it “inaccurately creates the appearance that the University is endorsing, supporting or affiliated with any organization, product, service, statement, or position?”**

This concept is reflected in other University policies that also require members of the University community to carefully differentiate their official activities from their personal activities and to make clear that, when speaking as private citizens, they do not act on behalf of the University.¹

When someone sends messages or publishes online from the msu.edu Internet domain, MSU’s identity becomes intertwined with the content in a way that may raise questions about whether MSU endorses the content. The easiest way to avoid such confusion is to use non-University IT resources whenever you engage in private, i.e., non-University, activities.

5. **Does MSU routinely monitor my use of MSU IT resources?**

MSU and its systems administrators do not routinely monitor individual use of IT resources or actively seek out User violations of the AUP. The University does, however, engage in activities necessary to protect the security and integrity of its IT resources. Practical and effective means by which the University identifies security threats include using automated tools to watch for unusual resource use patterns by individual User accounts and malware and other attack “signatures.” Sometimes these use patterns or signatures expose User activities that are in violation of the AUP. When this occurs, a follow-up investigation may result.

Current practices with respect to illegal sharing of copyrighted music, movie, or video files provide a useful illustration of this point. The University does not presently employ tools or techniques to seek out and identify people who are doing this on the MSU network. However, the University will investigate if a triggering event occurs. Examples of triggering events include a copyright owner or its agent filing a complaint; the use of a disproportionate amount of local network bandwidth by a User (Section 3.5) that is impeding others’ use of the network; or an employee’s workstation running out of storage space and local IT administrators finding that it is due to the storage of illicit files.

This same approach is in place with respect to the use of MSU IT resources to store, display, or disseminate pornography or other sexually explicit materials. While the University does not presently employ any techniques to seek out and identify people who are doing this on MSU IT resources, it will investigate if a triggering event occurs. Examples of triggering events include complaints from co-workers who have been subjected to pornographic images in the workplace; the use of a disproportionate amount of local network bandwidth by a User (Section 3.5) that is impeding others’ use of the network; or an employee’s workstation running out of storage space and local IT administrators finding that it is due to the storage of pornographic files.

¹ For example, see:
http://www.hr.msu.edu/documents/facacadhandbooks/facultyhandbook/AcademicFreedom.htm
http://www.hr.msu.edu/documents/facacadhandbooks/facultyhandbook/facultyrights.htm and
http://splife.studentlife.msu.edu/academic-freedom-for-students-at-michigan-state-university.
6. **What constitutes an “unreasonable” interference by one User with other Users’ use of MSU IT resources?**

In the context of limited IT resources, interference with other Users’ access to or use of a service by one User may arise when one User places a disproportionate burden or load on a system with limited service capacity. An example of “reasonable” interference might be when a single User makes a legitimate query of a database that temporarily consumes the majority of the system’s processing capacity, slowing or blocking the work of other Users. Such interference would be “unreasonable” if the same User did this repeatedly or was careless in formulating the most efficient query to meet the User’s needs.

7. **Why are there restrictions on fund raising, advertising, soliciting, and partisan political activities?**

Restrictions on use of IT resources for partisan political purposes are based on state and federal law. For example, with certain very limited exceptions, the Michigan Campaign Finance Act prohibits a public body like MSU or an individual acting for a public body like MSU from using public resources to assist, oppose, or influence the nomination or election of a candidate for public office or the qualification, passage, or defeat of a ballot question. (A “ballot question” is a question that is submitted or that is intended to be submitted to a popular vote at an election, whether or not it qualifies for the ballot.)

The Internal Revenue Code places even stronger restrictions on participation in campaigns for public office by tax-exempt organizations like MSU and their representatives. This provides the basis for the distinction between Section 3.7.1. and Section 3.7.2. Additional information on this topic may be found on the Office of the Vice President for Governmental Affairs website in the document titled *Information on Participation in Campaigns for Public Office and Ballot Measures: The University, University Employees, and other Members of the University Community.*

Other restrictions, such as incidental personal use for advertising, soliciting, or fund raising, are based on the likelihood that such personal activities will cause confusion or competition with the University’s own activities.

8. **May a MSU faculty member use MSU IT resources to engage in activities which have been approved under MSU’s Outside Work for Pay policy?**

It depends. The faculty Outside Work for Pay Policy states: “When engaged in outside work for pay, faculty members must make it clear that (a) they are acting in their individual capacities and not on behalf of the University; and (b) that the University does not endorse, sponsor, or support the outside work.”

The faculty policy also states: “University facilities, supplies and materials, equipment, services, or employees may be used for outside work for pay, but only if (a) such use would not be contrary to University policy or collective bargaining agreements, (b) such use would not adversely affect the use or availability of such facilities, supplies and materials, equipment, services, or personnel for unit and other University activities and operations; and (c) the University is reimbursed in full for the fair market value of the use of the facilities, supplies and materials, equipment, services, or employees.” Any
9. Why can’t someone use MSU IT resources to help out another organization, especially one that supports a good cause, just because it’s not affiliated with the University?

As a public institution, MSU must take care that its stewardship of its resources will withstand public scrutiny. MSU IT resources should not be used, just because they are available, to support non-affiliated organizations that should be acquiring their own IT resources, especially when IT resources are easily available outside the University, as they now are.

10. May MSU IT resources be used to support a professional organization or scholarly publication that exists outside MSU?

Generally yes. The great majority of professional organizations to which the University and members of the University community belong exist to promote missions which are consonant with the University’s goals. Similarly, the dissemination of scholarship is an important part of the University’s mission which professional journals also serve. Because of the considerations noted in FAQ 9, however, Section 3.9 of the Policy requires that the User first obtain approval for such uses from the University. For faculty, approval should be obtained from the relevant department chair/separately reporting director. For staff, approval should be obtained from the unit supervisor. Students or student groups may obtain approval from the Vice President for Student Affairs and Services.

11. I’m using my own personally-owned computer when I access MSU’s IT resources. If I don’t use “safe computing” practices on my own device, how does that hurt MSU and other users?

Security weaknesses in any one device or piece of software connected to the MSU network may present a security threat to all devices and services connected to the network. The “public health” of the network, just like the public health of communities, requires that individuals follow sound security practices with their own devices, software, and activities.

For network security purposes, the University may need to scan software or stored data on devices connecting to the MSU network, whether those devices are owned by the University or privately. Pursuant to Sections 5 and 6 of the Policy, the University will, insofar as possible limit such scanning in scope, time, and frequency; employ it to address specific security threats; and conduct it “robotically” (i.e., using software tools) rather than via direct human scrutiny of personal accounts.

12. If I violate the AUP or a local rule and my access to MSU IT resources is limited, suspended, or terminated, how quickly may I get it restored?

The timeframe for restoration of use privileges will depend on the seriousness of the violation. For example, a computer that has been blocked from accessing a network because the computer is harboring malware not intentionally installed by the owner (i.e.,
an “infected” computer) that is attacking systems or devices may have the block
removed as soon as the user can show network administrators that the malware has
been eradicated. At another extreme, a User who has intentionally committed a
particularly egregious AUP violation may lose privileges indefinitely.

13. What are examples of a User’s “electronic records”?

A “User’s electronic records” include, but are not limited to, e-mail, administrative
accounts, and network traffic, and also the devices on which these are stored or
processed.

14. May a University academic or administrative unit use “live” data in the
development or testing of a new service?

Sometimes it is necessary for a quantity of “live” data (i.e., active records) to be used to
develop or test a new service, software, or system. In these instances, the approval of
the VPLCT or his/her designee should be sought prior to the use to assure that proper
security measures are being taken to appropriately protect the privacy of the individuals
whose data are involved. Prior to granting approval, the VPLCT will consult with the
University offices that are the official stewards of the subject data type. Only University
organizational units may undertake this sort of data use; individual Users may not use
live data for these purposes except when they are acting on behalf of a University unit.

15. What are some examples of the types of situations referred to by Section
6.2.2.5 of the Policy?

The University might disclose User information to the police in cases where a student
has been reported missing and law enforcement personnel are investigating the matter.
The University might be compelled to disclose User information to defend against a
lawsuit that has been filed against the University.

16. Does Section 6.1.3 of the Policy mean that the University might disclose my
personal emails or other personal documents in response to a FOIA request?

The University's position is that personal electronic records of faculty, staff, and students
are not “public records” under the Michigan Freedom of Information Act. Users should
be aware, however, that such a determination may ultimately rest with a court of law
and not with the University. Therefore, Users are strongly encouraged to store their
personal documents and communications on personal devices and third party email
accounts rather than on MSU IT Resources.