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 a 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

use of MSU IT resources for outside work for pay must comply with these policy provisions.

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.

Acceptable Use Policy for MSU Information Technology Resources

(Administrative Ruling)

DRAFT, 27 September 2011

A trusted and effective information technology environment ("IT environment") is vital to the mission of Michigan State University. To that end, the University provides an IT environment which includes an array of institutional electronic business systems, computing services, networks, databases, and other resources (collectively, "MSU IT resources" or "resources"). These resources are intended to support the scholarship and work activities of members of the University's academic community and their external collaborators, to support the operations of the University, and to provide access to services of the University and other publicly available information.

Access to and usage of MSU IT resources entails certain expectations and responsibilities for both users and managers of the IT environment. These are stated below.

1. APPLICABILITY

1.1. This Policy applies to all individuals who use MSU IT resources ("Users"), regardless of affiliation and irrespective of whether those resources are accessed from MSU's campus or from remote locations.

1.2. Within MSU's IT environment, additional rules may apply to specific computers, computer systems or facilities, software applications, databases and data sources, data types, or networks, and to the uses thereof, or to local workplaces, or to specific types of activities (collectively, "local rules"). Local rules must be consistent with this Policy, but also may impose additional or more specific requirements or responsibilities on Users.

1.3. Users will be notified of, or given ready access (e.g., on a website) to, this Policy and any local rules that govern use of MSU IT resources.

2. PURPOSES AND APPROPRIATE USES

2.1. MSU IT resources are provided for University-related purposes, including support for the University's teaching, research, and public service missions, its administrative functions, and student and campus life activities.

2.2. Users are granted access to MSU IT resources for the purposes described in this Policy. Use should be limited to those purposes, subject to Section 2.3.

2.3. Incidental personal use.

2.3.1. Users may make incidental personal use of MSU IT resources, provided that such use is subject to and consistent with this Policy, including Article 3 of this Policy. In addition, incidental personal use of MSU IT resources by an MSU employee may not interfere with the fulfillment of that employee's job responsibilities or disrupt the work environment. Incidental personal use that inaccurately creates the appearance that the University is endorsing, supporting, or affiliated with any organization, product, service, statement, or position is prohibited.

2.3.2. Users who make incidental personal use of MSU IT resources do so at their own risk. The University cannot guarantee the security or continued operation of any MSU IT resource.

3. USER RESPONSIBILITIES

3.1. Users are responsible for informing themselves of any University policies, regulations, or other documents that govern the use of MSU IT resources prior to initiating the use of MSU IT resources.

3.2. Use of resources accessed through MSU IT resources.

3.2.1. When using MSU IT resources or resources owned by third parties that are accessed using MSU IT resources, users must comply with all applicable federal and state laws, all applicable University rules, ordinances, and policies, and the terms of any contract or license which governs the use of the third-party resource and by which the User or the University is bound.

3.2.2. In amplification and not in limitation of the foregoing, Users must not utilize MSU IT resources to violate copyright, patent, trademark, or other intellectual property rights.

3.3. Users may not engage in unauthorized use of MSU IT resources, regardless of whether the resource used is securely protected against unauthorized use.

3.4. Privacy of other Users.

3.4.1. Users are expected to respect the privacy of other Users, even if the devices and systems by which other Users access MSU's IT resources, the content other Users place on MSU IT resources, or the identities and privileges (rights to access and use certain systems and/or data), of other Users are not securely protected.

3.4.2. Unauthorized use by a User of another User's personal identity or access (log-in) credentials is prohibited.

3.5. MSU IT resources have a finite capacity. Users should limit their use of MSU IT resources accordingly and must abide by any limits MSU places on the use of its IT resources or on the use of any specific IT resource. In particular, no User may use any IT resource in a manner which interferes unreasonably with the activities of the University or of other Users.

3.6. MSU IT resources may not be used to fund raise, advertise, or solicit unless that use is approved in advance by the University.

3.7. Partisan political activities.

3.7.1. MSU IT resources may not be used to engage in partisan political activities on behalf of, or in opposition to, a candidate for public office.

3.7.2. MSU IT resources may not be used to promote or oppose the qualification, passage, or defeat of a ballot question that does not affect the University's interests. MSU IT resources may not be used to promote or oppose the qualification, passage, or defeat of a ballot question that affects the University's interests unless that use is approved in advance by the President.

3.8. MSU IT resources may not be used to operate a business or for commercial purposes unless that use is approved in advance by the University.

3.9. MSU IT resources may not be used to support the operations or activities of organizations that are not affiliated with the University unless that use is approved in advance by the University.

3.10. Pornography and sexually explicit content.

3.10.1. Unless such use is for a scholarly or medical purpose or pursuant to a formal University investigation, Users may not utilize MSU IT resources to store, display, or disseminate pornographic or other sexually explicit content. This prohibition does not apply to private computers that are attached to the University's network.

3.10.2. Child pornography is illegal. The use of MSU IT resources to store, display, or disseminate child pornography is absolutely prohibited. Any such use must be reported immediately to the MSU Police Department.

3.11. In operating its IT environment, the University expects Users to engage in "safe computing" practices, such as establishing appropriate access restrictions for their accounts, setting strong passwords and guarding those passwords, keeping their personal operating systems and software applications up-to-date and patched, and employing security measures on their personal devices.

4. ENFORCEMENT

4.1. Use of MSU IT resources is a privilege and not a right. A User's access to MSU IT resources may be limited, suspended, or terminated if that User violates this Policy. Alleged violations of this Policy will be addressed by the Director of Academic Technology Services (ATS) or his/her designee.

4.2. Users who violate this Policy, other University policies, or external laws may also be subject to disciplinary action and/or other penalties. Disciplinary action for violation of this Policy is handled through the University's normal student and employee disciplinary procedures.

4.3. In addition to its own administrative review of possible violations of this Policy and other University policies, the University may be obligated to report certain uses of MSU IT resources to law enforcement agencies. See, e.g., Section 3.10.2.

4.4. If the Director of ATS determines that a User has violated this Policy and limits, suspends, or terminates the User's access to any MSU IT resource as a result, the User may appeal that decision to the Vice Provost for Libraries, Computing and Technology ("VPLCT"). If the User believes that his/her appeal has not been appropriately addressed by the VPLCT, he/she may seek further redress as follows:

4.4.1. if an undergraduate student, through the Vice President for Student Affairs, or his/her designee;

4.4.2. if a graduate or professional student, through the Dean of the Graduate School, or his/her designee;

4.4.3. if a member of the faculty or academic staff, through the Associate Provost and Associate Vice President for Academic Human Resources, or his/her designee;

4.4.4. if an employee covered by a collective bargaining agreement, through the Director of Employee Relations, or his/her designee.

4.5. Alleged violations of local rules will be handled by the local systems administrator, network administrator, or employee supervisor/unit manager, depending on the seriousness of the alleged violation. These individuals will inform and consult with the Director of ATS or his/her designee regarding each alleged violation of a local rule and the appropriate consequences for any violation of a local rule. Users who object to the limitation, suspension, or termination of their access to any MSU IT resource as a consequence of their violation of a local rule may appeal to the VPLCT.

4.6. The VPLCT may temporarily suspend or deny a User's access to MSU IT resources when he/she determines that such action is necessary to protect

such resources, the University, or other Users from harm. In such cases, the VPLCT will promptly inform other University administrative offices, as appropriate, of that action. Local MSU IT resource administrators may suspend or deny a User's access to the local resources they administer for the same reasons without the prior review and approval of the VPLCT, provided that they immediately notify the Director of ATS and the VPLCT of that action.

5. SECURITY AND OPERATIONS

5.1. The University may, without further notice to Users, take any action it deems necessary to protect the interests of the University and to maintain the stability, security, and operational effectiveness of its IT resources. Such actions may be taken at the institutional or local level, and may include, but are not limited to, the scanning, sanitizing, or monitoring of stored data, network traffic, usage patterns, and other uses of its information technology, and blockade of unauthorized access to, and unauthorized uses of, its networks, systems, and data. Local and central institutional IT resource administrators may take such actions in regard to the resources they manage without the prior review and approval of the VPLCT.

6. PRIVACY

6.1. General provisions:

6.1.1. Responsible authorities at all levels of the MSU IT environment will perform management tasks in a manner that is respectful of individual privacy and promotes User trust.

6.1.2. Monitoring and Routine System Maintenance

6.1.2.1. While the University does not routinely monitor individual usage of its IT resources, the normal operation and maintenance of those resources requires the backup of data, the logging of activity, the monitoring of general usage patterns, and other such activities. The University may access IT resources as necessary for system maintenance, including security measures.

6.1.2.2. The University's routine operation of its IT resources may result in the creation of log files and other records about usage. This information is necessary to analyze trends, balance traffic, and perform other essential administrative tasks. The creation and analysis of this information may occur at central institutional and local levels.

6.1.2.3. The University may, without further notice, use security tools and network and systems monitoring hardware and software.

6.1.3. The University may be compelled to disclose Users' electronic records in response to various legal requirements, including subpoenas, court orders, search warrants, discovery requests in litigation, and requests for public records under the Michigan Freedom of Information Act ("MIFOIA").

6.1.4. The University reserves the right to monitor and inspect Users' records, accounts, and devices as needed to fulfill its legal obligations and to operate and administer any MSU IT resource.

6.1.5. The University may disclose the results of any general or individual monitoring or inspection of any User's record, account, or device to appropriate University authorities and law enforcement agencies. The University may also use these results in its disciplinary proceedings.

6.2. Provisions regarding inspections and disclosure of personal information:

6.2.1. General provisions.

6.2.1.1. In order to protect User privacy, the VPLCT or his/her designee must review and approve *any* request for access by a person to an individual User's personal communications or electronically stored information within MSU IT resources.

6.2.1.2. Incidental access to the contents of an individual User's personal communications or electronically stored information resulting from system operational requirements described elsewhere in this Policy does not require the prior review and approval of the VPLCT.

6.2.2. The University, acting through the VPLCT, may access or permit access to the contents of communications or electronically stored information:

6.2.2.1. When so required by law. If necessary to comply with the applicable legal requirement, such disclosures may occur without notice to the User and/or without the User's consent.

6.2.2.2. In connection with an investigation by the University or an external legal authority into any violation of law or of any University policy, rule, or ordinance. When the investigational process requires the preservation of the contents of a User's electronic records to prevent their destruction, the VPLCT may authorize such an action.

6.2.2.3. If it determines that access to information in an employee's electronic account or file is essential to the operational effectiveness of a University unit or program and the employee is unavailable or refuses to provide access to the information.

6.2.2.4. If it receives an appropriately prepared and presented written request for access to information from an immediate family member or the lawful representative of a deceased or incapacitated User.

6.2.2.5. If it must use or disclose personally identifiable information about Users without their consent to protect the health and well-being of students, employees, or other persons in emergency situations, or to preserve property from imminent loss or damage, or to prosecute or defend its legal actions and rights.