"DON'T SOCIALIZE YOURSELF OUT OF A JOB"

"USING SOCIAL MEDIA AT WORK"

And Other IT Issues

The Problem and Do's and Don'ts and Why Not

- 70% of 275 U.S. employers have rejected candidates based on information found online.
- 35% of those employers said they rejected applicants based on membership in certain groups.
- There is no privacy on the employers e-mail: E-mails sent through an employer's e-mail system legally may be viewed by the employer.
- E-mails sent through a public body's e-mail system may later be discoverable under the Freedom of Information Act.
    - While social networking sites allow a person to limit who can review their postings, all it takes is for one "friend" to share the information with someone else and the information is soon in the public domain.
- An Electronic Communication is forever. It can't be burned like a letter.

Some Practical Recommendations:

Consider restricting who you "friend" on Social Media.

- Students should be carefully considered especially if you supervise them. (If this were K-12 employees the recommendation would be never.)
- Employees you supervise should probably be avoided.
- Your boss – wait until you are one, too.

E-mail, Texts, Posts, Tweets, IMs, etc.

- If you are OK with your post going to everyone on campus, including your boss and the President, then post it. If not, run it by your friends or APA.

DO NOT post:

- Inappropriate, vulgar, or obscene language or materials
- Language or materials that could be considered inappropriate or unprofessional
- Photos which could be considered inappropriate or unprofessional

Before posting, sending e-mail or text message ask yourself:

- How would I like to see it on a Campus billboard? Sent to your mother? Your Boss? President Simon?

- Before sending a text message or e-mail, ask yourself, "How would this affect me if it became known to my supervisor, colleagues, or students?"

DON'T I HAVE FREE SPEECH RIGHTS UNDER THE 1ST AMENDMENT

Employee speech is <u>not</u> entitled to absolute First Amendment protection:

1) If the employee is merely speaking about matters of *personal concern*; or

2) If school officials believe that the employee's speech might *disrupt the workplace* or interfere with the performance of his or her job; or

3) The statements are false or made in reckless disregard of their truth or falsity.

-Education Employee was fired after being convicted of 3 counts of allowing a minor to possess alcohol after a Facebook picture of the employee with 3 underage students holding Smirnoff bottles.

-Fire chief was terminated for website containing publicly available pension information with the statement "protect our pensions." Employer is arguing that the chief lost sight of his role as part of the management team in union negotiations.

Students are protected by First Amendment more than Employees

Students have the 1st Amendment right to post disparaging comments about education employees including opinions that the employee is the worst instructor unless it causes classroom disruption.

DON'T I HAVE A RIGHT TO PRIVACY UNDER THE 1ST AMENDMENT

Courts use a 4 factor test to determine if the employee has a reasonable expectation of privacy in electronic communication:

1. Does ER have a policy that bands personal or other objectionable use of e-mail?
2. Does ER monitor employees' use of computer or e-mail?
3. Do third parties have access to the e-mails, internet or computer?
4. Does the ER notify or make the EEs aware of use and monitoring policies.
5. If the policy is not clear, then the nature of the e-mail may create greater right such as attorney client privilege.

You may have protection if:

-The employer accesses messages sent over personal email accounts over employer owned computers but relies on the acceptable use policy where employees were given a reasonable expectation of privacy. MSU employees do not have a reasonable expectation of privacy.

-The employer inspects communications made through an employer owned computer kept at the employee's home or worked from home on regular basis.

-The employer allows some personal use but conditions use on "the highest standards of morality" or other imprecise standards.

-The employer disciplines an employee for electronic communications made outside of working hours and not through the employer systems.

-The employer disciplines an employee in violation of an acceptable use policy or collective bargaining agreement.

LITIGATION HOLD – THERE IS A DUTY TO PRESERVE EVIDENCE WHEN A PARTY REASONABLY ANTICIPATES LITIGATION.

-Reasonable anticipation of litigation requires suspension of an employer's routine document retention/destruction policy to ensure preservation of relevant documents.

-FOIA request, accident, complaint, law suit or threat of suit, investigation trigger the hold.

-Includes e-mail, databases, pictures, paper, digital and electronic formats.

-Any person who willfully destroys records under litigation hold may be guilty of a crime.

-Destruction may result in court sanctions.

-Destruction may result in adverse inference in litigation, i.e. the jury may assume that the reason the documents were destroyed is because they hurt the defendant's case.

NLRB POSITION ON EMPLOYER WORK RULES

Employee Rights Under PERA and NLRA

It shall be lawful for public employees to organize together or to form, join or assist in labor organizations, to engage in lawful concerted activities for the purpose of collective negotiation or bargaining or other mutual aid and protection, or to negotiate or bargain collectively with their public employers through representatives of their own free choice..." "…for purposes of collective bargaining in respect to rates of pay, wages, hours of employment or other conditions of employment."

Acceptable Use – Policies & Work Rules

An employer violates Section 8(a)(1) through the maintenance of a work rule if that rule "would reasonably tend to chill employees in the exercise of their Section 7 rights." Lafayette Park Hotel, 326 NLRB 824, 825 (1998), enfd. 203 F.3d 52 (D.C. Cir. 1999). The Board uses a two step inquiry to determine if a work rule would have such an effect. Lutheran Heritage Village–Livonia, 343 NLRB 646, 647 (2004).

First, a rule is clearly unlawful if it explicitly restricts Section 7 protected activities. If the rule does not explicitly restrict protected activities, it will only violate Section 8(a)(1) upon a showing that:(1) employees would reasonably construe the language to prohibit Section 7 activity; (2) the rule was promulgated in response to union activity; **or** (3) the rule has been applied to restrict the exercise of Section 7 rights.

An Employee Cannot Be Disciplined For Concerted Protected Activity

An activity is concerted when an employee acts "with or on the authority of other employees and not solely by and on behalf of the employee himself." The definition of concerted activity "encompasses those circumstances where individual employees seek to initiate or to induce or to prepare for group action."

Protected Activity

An employer probably violates the law if it disciplines an employee for concerted protected activity unless that activity is done while at work during work time and thus interferes with completion of work.

Safe way to be sure, is to make it a subject addressed with APA through e-mail or website.

NLRB Cases

-Work rule prohibiting employees from "disparaging" the employer in any media unlawful.

Employee of same employer was fired after posting with expletives that the employer messed up and she was done being a good employee where she was friends with 10 coworkers including her direct supervisor. Other employees made similar comments. NLRB held the discharge violated NLRA because the action was about working conditions and was concerted.

-Discharge for Facebook comments lawful but social media policy unlawful.

Discharge did not violate act because employee not engaged in protected activity where she posted on Facebook during a work break "F&*# (name of employer)" to which 1 coworker and 3 friends "liked" and two non-employees commented. 30 minutes later she posted again that the employer "doesn't appreciate its employees." Several friends and relatives commented but no coworkers. She was discharged after asking to explain her Facebook postings and NLRB said comments were not in concert with other employees but just an individual gripe.

5 days later the employer issued a new social media policy "in external social networking situations, employees should generally avoid identifying themselves as the Employer's employees, unless there was a legitimate business reason to do so or when discussing terms and conditions of employment in an appropriate manner." NLRB held the policy was unlawful.

-

-**Suggestion** – if you see a fellow employee griping about the employer on social media, forward to APA and suggest that it is a wider problem and the union should address it.

Michigan Compiled Laws MCL 752.795 Prohibited conduct.

Sec. 5. A person shall not intentionally and without authorization or by exceeding valid authorization do any of the following:

> (a) Access or cause access to be made to a computer program, computer, computer system, or computer network to acquire, alter, damage, delete, or destroy property or otherwise use the service of a computer program, computer, computer system, or computer network.
>
> (b) Insert or attach or knowingly create the opportunity for an unknowing and unwanted insertion or attachment of a set of instructions or a computer program into a computer program, computer, computer system, or computer network, that is intended to acquire, alter, damage, delete, disrupt, or destroy property or otherwise use the services of a computer program, computer, computer system, or computer network. This subdivision does not prohibit conduct protected under section 5 of article I of the state constitution of 1963 or under the first amendment of the constitution of the United States.

Michigan v. Leon Jermane Walker**,** ____Mich App ___, (Dec 27, 2011)
http://coa.courts.mi.gov/documents/opinions/final/coa/20111227_c304593_54_304593.opn.pdf

An Oakland County IT tech was convicted of a felony for violating this law by accessing his wife's e-mail account that was password protected and the Michigan court of appeals upheld the conviction. Even after he was charged, Mr. Walker misled employees of Oakland County into allowing him access to CLEMIS (Court and Law Enforcement Management Information System) which resulted in a second charge and conviction.

HBs 4508 and 4532 both would retroactively make his access of wife's email legal.

. U.S. STORED COMMUNICATIONS ACT – Criminal Penalties

18 U.S.C. §2701. Unlawful access to stored communications

(a) Offense.—**Except as provided in subsection (c) of this section whoever**—

(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or

(2) **intentionally exceeds an authorization to access that facility;**

and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system shall be punished as provided in subsection (b) of this section.

(b) Punishment.—**The punishment for an offense under subsection (a) of this section is**—

(1) **if** the offense is **committed for** purposes of **commercial advantage, malicious destruction or damage, or private commercial gain**, or in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or any State—

(A**) a fine** under this title **or imprisonment for not more than 5 years**, **or both**, in the case of a first offense under this subparagraph; and

(B) a fine under this title or imprisonment for not more than 10 years, or both, for any subsequent offense under this subparagraph; and

(2**) in any other case**—

(A) **a fine** under this title or **imprisonment for not more than 1 year or both**, in the case of a first offense under this paragraph; and

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under this subparagraph that occurs after a conviction of another offense under this section.

(c) Exceptions.—Subsection (a) of this section **does not apply with respect to conduct authorized**—

(1) **by the person or entity providing a wire or electronic communications service**;

(2) **by a user of that service with respect to a communication of or intended for that user**; or

(3) in section 2703, 2704 or 2518 of this title (access by a government entity by warrant/subpoena of electronic document or back up tape, or wiretap by warrant)

§2707. Civil action

(a) Cause of Action.—Except as provided in section 2703(e**), any** provider of electronic communication service, subscriber, or other **person aggrieved by any violation of this chapter** in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind **may, in a civil action, recover from the person** or entity, other than the United States, **which engaged in that violation** such relief as may be appropriate.

(b) Relief.—In a civil action under this section, **appropriate relief includes**—

(1) such preliminary and other **equitable or declaratory relief** as may be appropriate;

(2) **damages** under subsection (c); and

(3) a **reasonable attorney's fee and other litigation costs** reasonably incurred.

United States v Batti, U.S. Court of Appeals Sixth Circuit, ____F3rd_____ (Jan 14, 2011)
http://caselaw.findlaw.com/us-6th-circuit/1552671.html

Criminal defendant worked in the IT department of Campbell Ewald, a Michigan advertising company. After he was fired he took confidential computer files that he had accessed 6 months earlier without permission. The 6th Circuit upheld the enhanced felony conviction based upon the employer's cost in investigating the employee. The court upheld the conviction and restitution of $47,565.

Brian Pietrylo et al. v Hillstone Restaurant Group, U.S. District Court, New Jersey
http://www.employerlawreport.com/uploads/file/PIETRYLO%20v%20%20HILLSIDE%20RESTAURANT.pdf

Employees created a private MySpace website via invitation only to vent about work. Hillstone found out, asked or coerced an employee into providing access to the site and fired several employees. The employees sued under the Stored Communications Act and similar State Law. A federal jury awarded back pay and $13,600 in punitive damages.

ACCEPTABLE USE POLICY (AUP)
FOR MSU INFORMATION TECHNOLOGY RESOURCES

Frequently Asked Questions (FAQ)

1. Why is the AUP being revised?

The current AUP was last revised in the summer of 1992. In 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 the "local" rules to which Section 1.2 of the Policy refers 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 minimis* 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. Can I use MSU IT resources to access Facebook or other social media for private (non-University) reasons?

Yes, as long as these activities comport with the limits on "incidental personal use" described in Section 2.3 of the Policy. In other words, while the University does not prohibit the use of its IT resources to engage in social media for non-University reasons, it will not permit abuse of this privilege. For example, extensive personal use of social media during work hours (using MSU IT resources or not) may well disrupt the work environment or interfere with an employee's job performance, which is prohibited by Section 2.3.1. If that occurs, it will be addressed by the unit supervisor as a personnel issue.

6. What other laws and policies besides the Acceptable Use Policy govern the use of MSU IT resources?

[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.

Section 3.2.1 of the Policy requires Users to comply with all applicable federal and state laws and all applicable University rules, ordinances, and policies. This means that Users who are employees and students of MSU are subject to the other policies and rules of the University when they use MSU IT resources. So, if a use of MSU IT resources violates another University rule or policy, like one of the General Student Regulations or the Sexual Harassment Policy, the User may be sanctioned through the appropriate student or employee disciplinary procedure (see Section 4.2), as well as risking loss of access to MSU IT resources under Section 4.1 of the Policy.

Users may be held responsible by the relevant external legal authorities for the use of MSU IT resources to violate federal and state laws. Such violations may be criminal (e.g., child pornography, stalking) or civil (e.g., defamation, invasion of privacy) in nature. While the University may provide access to personal communications or electronically stored information in connection with an investigation or adjudication of alleged violations of external law (see Sections 4.3, 6.1.3-5, and 6.2 of the Policy), if the User who allegedly violates the external law is not an MSU employee acting within the scope of his or her employment or an MSU student whose conduct would also violate an MSU policy or rule, the University will generally defer to external legal and judicial authorities as the appropriate forums for the resolution of such matters.

7. Does MSU routinely monitor my use of MSU IT resources? What are MSU's typical practices for detecting and investigating possible violations of the AUP?

MSU and its systems administrators do not routinely monitor individual use of IT resources or actively seek out User violations of the AUP. Generally, the University does not undertake investigations without a triggering event such as a complaint or a technical system or service performance problem. For example, 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 another 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 runs out of storage space because it turns out to be full of illicit files.

Similarly, while the University does not presently employ any techniques to seek out and identify people who are storing, displaying, or disseminating pornography or other sexually explicit materials 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 runs out of storage space because it is full of pornographic files.

8. Under Section 3.5, what constitutes an "unreasonable" interference by one User with other Users' use of MSU IT resources?

When one User places a disproportionate burden or load on a system with limited service capacity, like the University's, that User may interfere with other Users' access to or use of the system. 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. Another example might be transferring a very large data file, such that the bandwidth of certain network segments is largely consumed by one User, which slows or blocks 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 or data transfer mechanisms to meet the User's needs.

9. 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 those on use of MSU IT Resources 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.

10. Can I use MSU IT resources to engage in any activities related to campaigns for public office and ballot questions without violating this Policy?

Yes. The following are examples of activities related to campaigns for public office and ballot questions for which members of the University community may use MSU IT resources without violating this Policy:

- Engaging in scholarly research about past or current political campaigns or the issues that underlie them.
- Disseminating the results of such research in a manner consistent with normal academic practice.
- Issuing invitations from a student organization to guest speakers or candidates, provided that speakers on both sides of a ballot initiative and all candidates for a public office have equal opportunities to appear on campus.
- Engaging in nonpartisan educational activities related to ballot measures or to political campaigns. (See Governmental Affairs website for specific examples.)
- Hosting political activities at apartments or residence hall rooms of individuals who reside in University housing, as long as the residence is not used for a political fund-raising event.
- Researching or communicating about pending legislation.

11. Can a faculty member use MSU IT resources in connection with course assignments that require student involvement in campaign activities?

Yes. University faculty and students may use MSU IT resources in connection with course assignments that require student involvement in campaign activities, as long as the faculty member does not specify the candidates or ballot measures on whose behalf the students should campaign and where, for example, students write papers or make class presentations evaluating their experiences.

12. Can registered student organizations continue to conduct fund-raising activities using MSU IT Resources?

Yes. The revised Policy has not altered the current rules regarding fund-raising by registered student organizations. (RSOs are considered "affiliated with the University" for purposes of Section 3.9.) RSOs should continue to follow the normal approval process for conducting fund-raising activities. Questions about that process should be directed to the Department of Student Life.

13. 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.

14. 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. (See FAQ 9 for more on this topic.)

15. 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 that 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.

16. How does this Policy affect academic assignments and projects that might have the effect of supporting a business or professional organization?

The Policy does not interfere with a faculty member's ability to assign academic projects that might benefit a business or professional organization, or a student's use of MSU IT resources while participating in an academically-approved internship or similar experience with a business or organization outside of MSU . Such assignments are commonplace in certain campus units, such as the Broad College of Business. If faculty members are unclear about the appropriateness of a particular assignment under this or any other University policy, they are encouraged to seek guidance from the Office of the Provost.

17. 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.

18. 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.

19. What are examples of a User's "electronic records" referred to by Section 6.1.3 of the Policy?

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.

20. 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.

21. 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.

22. 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.

23. My MSU email address is my only email address and I use it for everything. Can I continue to do that?

Yes, although it is not recommended. Numerous free and easy-to-use alternatives are now available to the public, and Users are strongly encouraged to set up an alternative email account for personal use. A User who chooses to continue using his/her MSU account for both personal and business purposes should create a "personal" folder within the MSU account to store personal items. Segregating personal and business items will enhance the privacy of items contained within the personal folder and mitigate against unintentional access to those personal items. Users may not store University records or data in personal folders.

24. How often will this Policy be reviewed?

The Office of the Vice Provost for Libraries, Computing & Technology will periodically review the Policy to assure that it reflects best practices and is in compliance with applicable laws and regulations. Such reviews are expected to occur no less frequently than once every three years. Reviews may, of course, occur more frequently, if circumstances require, and will include input from the appropriate academic governance committees.

25. What are examples of the "private devices attached to the University's network" to which Sections 3.7.3 and 3.10.1 refer?

A "private device" means a privately-owned computer, tablet, smartphone, etc., that is connected to and using the University's network to move data, messages, voice or video signals, etc. between itself and the Internet. The prohibition of Section 3.10.1 does not apply when the sole use of MSU IT resources is this network-communications use involving a private device. Nor, in similar circumstances, do the prohibitions in Section 3.7, assuming the message conveyed across the University's network from the private device does not suggest that the University endorses or supports that message (e.g., by use of the msu.edu Internet domain).

MSU ACCEPTABLE USE POLICY
Acceptable Use Policy for
MSU Information Technology Resources

(Administrative Ruling)

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 using MSU IT resources ("Users"), regardless of affiliation and irrespective of whether these 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 to (e.g., on a website), this Policy and 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.

3.7.3. These prohibitions do not apply to private devices that are attached to the University's network, provided that MSU IT resources are not used in a way that suggests the University endorses or supports the activity originating on the private device.

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 devices 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, 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 as long as the actions involve automated tools and not direct human inspection.

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.