THE UNIVERSITY OF MICHIGAN

STANDARD PRACTICE GUIDE

SECTION:	General University Policies	**Number:**	601.11
		Revised:	9/7/2004
SUBJECT:	Privacy and the Need to Monitor and Access Records	**Date Issued:**	12/1/93
		Review Date:	9/7/08
		Attachment(s)	0
APPLIES TO:	All Employees		
ISSUED BY:	Provost and Executive Vice President for Academic Affairs		

I. Background

The University of Michigan respects the privacy of its employees and seeks to foster a climate free from arbitrary or capricious monitoring of employees and the *records*[1] they create, use, or control.

Nonetheless, the University must, at times, access *records* or monitor *record systems* that are under the control of its employees. Furthermore, because the University permits some latitude for employees to use University resources to conduct University business off-campus and to conduct personal matters at their work sites, *work-related records* and employees' *personal records* may be located in the same place.

This policy defines the rights, responsibilities, and expectations of the University and its employees regarding the conditions under which they may access *records* and monitor *record systems*.

II. Policy

There are many laws that govern the maintenance and disclosure of *records*. Federal and state laws, for example, require the University to:

- protect from unwarranted disclosure certain *records* of patients (HIPAA), students (FERPA), or library patrons (Michigan Library Privacy Act);
- disclose *records* (Freedom of Information Act, see **http://www.umich.edu/~urel/foia.html**, subpoenas, etc.); and/or
- monitor *record systems*.

Accordingly, the University of Michigan cannot guarantee the privacy of any *records*, including the *personal records*, of any University employee.

This policy governs those circumstances in which the University, when not governed by external law, will monitor or access *records* and *record systems*.

Other than as authorized under the regulations of this policy, neither the University nor any employee acting on behalf of the University will access *records* or monitor the content of *record systems*

[1] Words that appear in *italics* are defined in section VI, Definitions.

located on University-controlled premises or University property, which includes but is not limited to University computers, networks, offices, and telephones.

III. Regulations

A. University Obligations

1. Standards for Accessing or Monitoring *Records*

As described below, the University has established general standards for accessing or monitoring all types of *records* (*business, faculty-owned scholarly*, and *personal*) or *record systems*, and additional standards for accessing or monitoring each type of *record*.

a. Standards that apply to all *business, faculty-owned scholarly,* and *personal records* or *record systems*

The University may access or monitor all *records (business, faculty-owned scholarly*, and *personal*) or *record systems* in the following circumstances:

1. When the University must monitor *record systems* to avert reasonably anticipated threats or hazards to those *record systems*. An example includes scanning to detect computer viruses. (This does not include an examination of the contents of *records* or *record systems.*); or

2. When the University is required by law to access, monitor, or disclose *records* or *record systems*.

b. Standards that apply to each type of *record (business, faculty-owned scholarly, and personal)*

1. *Business Records*

The University may access *business records* or monitor the *business record* content of *record systems* in the following circumstances:

- When the University has a *legitimate business need* to know or access the information contained in *business records,* and the employee who controls the *business records* or access to the *business records* (e.g. password, assigned office holder, etc.) is unavailable or unwilling to give consent to access.

2. *Faculty-Owned Scholarly Records*

According to the 1940 Statement of Principles on Academic Freedom and Tenure, American Association of University Professors' Policy Documents & Reports (1995 ed.), "Institutions of higher education are conducted for the common good and not to further the interest of either the individual teacher or the institution as a whole. The common good depends upon the free search for truth and its free expression."

Consistent with academic freedom and tradition, all University of Michigan faculty (including full-time, part-time, adjunct, and emeritus faculty) own and control instructional materials and scholarly works created at their own initiative with usual University resources. (For more information regarding ownership of works, see SPG section 601.03-2 "Ownership of Copyrighted Works Created at or in Affiliation with the University of Michigan.")

For the purposes of this policy the monitoring and access standards that apply to *faculty-owned scholarly records* (or *records* that are labeled as such) will also apply to *personal records.*

3. *Personal Records*

The University and its employees will not access or monitor the content of *personal records* (including *faculty-owned scholarly records*), or monitor the *personal records* (including *faculty-owned scholarly records*) content of *record systems*, except under the following circumstances:

a. When an employee who controls *faculty-owned scholarly* or *personal records* (e.g. password, assigned office holder, etc.) is unavailable or unwilling to give consent to access and when it is necessary for the University to determine whether there are *business records* contained therein, the University will access such *records* only to the extent necessary; or

b. When there is reasonable cause to believe that the employee has engaged in misconduct and may have used University resources improperly.

2. Preserving and Protecting *Records*

In circumstances where the University determines that there may be a specific risk to the integrity or security of *records*, the University may take measures to protect or preserve those *records*. For instance, the University may take a "snapshot" of a computing account to preserve its status on a given date, copy the contents of a file folder, or restrict access to a *record system*. The University may access or monitor preserved or protected *records* pursuant to Part III of this policy.

B. Employee Obligations

1. File Maintenance

a. *Work-Related Records*. Employees are responsible for organizing their *work-related records* so that they are accessible to those with a *legitimate business need* to know or access the information contained in them.

b. *Faculty-owned Scholarly* or *Personal Records*. While the University cannot provide an absolute guarantee as to the privacy of *faculty-owned scholarly* or *personal records*, employees should take reasonable measures to safeguard against inappropriate or inadvertent access to their *records*. Employees should mark as

"private" or "personal" all *personal records*, or as "scholarship" or "research" all *faculty-owned scholarly records* maintained on University-controlled premises or property. Employees should maintain this information in an identifiable separate location (e.g. folder or file) from their *business records*.

2. Standards of Employee Conduct for Accessing or Monitoring *Records*

It is a violation of this policy for an employee to monitor *record systems* or access *records* beyond the standards established by Section III. A. of this policy. It is also a violation of the policy if the University has granted access to the employee (to monitor or access *records*) and if the employee has accessed or monitored *records* or *record systems* for purposes other than the purposes for which the University has granted access.

IV. Sanctions

Violations of this policy will be considered misconduct on the part of the employee and will be subject to institutional sanctions up to and including termination of appointment.

Violations of this policy include:

1. An employee monitors *record systems* or accesses *records* beyond the standards established by Section III. A. of this policy.
2. The University has granted access to the employee (to monitor or access *records*) and the employee accesses or monitors *records* or *record systems* for purposes other than the purposes for which the University has granted access.

V. Employee Grievances

Employees who allege that the University has violated their rights as described in this policy may file a grievance under the appropriate University grievance procedure. Staff members should see Standard Practice Guide 201.08 "Grievance Procedures and Dispute Resolution" http://spg.umich.edu/pdf/201.08.pdf and faculty members should see the Faculty Handbook, Section 10.H "Formal Grievance Procedures" (http://www.provost.umich.edu/faculty/handbook/10/10.H.html); union members (faculty or staff) should refer to the grievance procedure in the applicable collective bargaining agreement.

VI. Definitions

A. Records

For purposes of this policy, a record is any document, file, computer program, database, image, recording, or other means of expressing fixed information that is created, received, used, or maintained within the scope of University business or employment at the University or that resides on University-controlled premises or property. Records are either *work-related* or *personal*.

B. Record Systems

Record systems are ways of storing, disseminating, or organizing *records*. They include, but are not limited to, computers, computing networks, telephones lines, voice mail, fax machines, filing cabinets, etc. which are University property or which are controlled by the University.

C. Work-Related Records

Work-related records are either *business records* or *scholarly records*.

D. Business Records

A business record is any *record* created, received, used, or maintained by an employee in the normal course of his or her professional responsibility or work for the University. This includes *records* relating to an employee's professional development, but does not include *faculty-owned scholarly records*. Examples of business records are drafts or final documents, including underlying or supporting documentation, of the following:

- budget reports;
- documents shared with or generated by third parties, such as purchase orders, bills for services or contracts with vendors;
- data sets that do not meet the definition of *faculty-owned scholarly records,* such as financial or enrollment data*;*
- feasibility studies or utilization analysis;
- attendance records, work schedules, or work orders;
- architectural drawings;
- correspondence or memoranda related to University business;
- course syllabi;
- student grades;
- meeting minutes;
- departmental web sites or e-mail groups; and
- committee reports.

E. Faculty-Owned Scholarly Records

Faculty-owned scholarly records are defined in SPG section 601.03-2 "Ownership of Copyrighted Works Created at or in Affiliation with the University of Michigan" as works that are created at the faculty member's own initiative with usual University resources. They include, but are not limited to *records* related to information gathering, knowledge production, methodology, distribution, handouts, reading lists, research, research plans, notes, charts, articles, presentations, books, scholarly commentary, consulting works, films, music, choreography, works of art, and all other *records* produced in the role of scholar, researcher, teacher, or faculty member. They do not include grades or course syllabi, nor do they include *records* produced using unusual University resources, commissioned works, or *records* created as a result of a faculty member's administrative appointment, or service to the University, such as committee work or serving as a hearing officer.

F. Personal Records

A personal record is a *record* that is created, received, used, or maintained by an employee for a purpose not related in any way to his or her work for the University.

G. Legitimate Business Need

A legitimate business need is any reason necessary to conduct the normal business of the University. A legitimate business need can be held only by a person who, based strictly on his or her job responsibilities, has a specific need to know the information accessed or monitored. The normal business of the University includes, but is not limited to:

- preparation of departmental budgets;
- ordering of materials, supplies, and equipment for the unit;
- activity related to providing service, such as food service, human resources, legal services, computer support services, etc.;
- strategic planning activity;
- planning, financing and construction of capital projects;
- preparation of work schedules;
- duties related to University committees; or
- audits of University finances, processes, and related activity.

Legitimate business need does ***not*** include access or monitoring the content of *records* or *record systems* in order to determine:

- whether a faculty or staff member is spending an excessive amount of work time on personal activities; or
- whether a faculty or staff member has committed misconduct, unless there is reasonable cause to believe that misconduct has been committed, ***and*** that University resources may have been used improperly.