

# Access and Compliance

Proper Use of University Information Systems

---

The University of Michigan-Flint  
Information Technology Services

# Access and Compliance

Proper Use of University Information Systems



## Table of Contents

Introduction.....	3
Using Information Correctly (Federal and State Acts) .....	3
The Family Education Rights and Privacy Act.....	3
The State of Michigan Freedom of Information Act .....	4
The Federal Freedom of Information Act and the Federal Privacy Act of 1974 .....	5
The Health Insurance Portability and Accountability Act of 1996 (HIPAA).....	5
Using Information Correctly (University Policy) .....	5
Bylaw of the Board of Regents.....	5
The Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan.....	6
The Institutional Data Resource Management Policy.....	6
The Proper Use of Information Technology at the University of Michigan-Flint.....	6
Applying Policies to the Information Systems .....	7
What Can You do to Secure the Data to which You have Access?.....	7
Information Misuse and Consequences .....	7
Examples of Violations.....	8
Consequences of Misuse.....	8
The Information Systems Access and Compliance Statement.....	9
Bibliography .....	10
Available from Information Technology Services.....	10
Available from the Information Technology Division .....	10
Available from the University Audits Office.....	10

## Introduction

This Access and Compliance document is designed to acquaint you with the policies that define and regulate responsible use of information at the University of Michigan-Flint.

It contains information about state and federal laws and regulations that have been adopted to protect individual privacy and how those regulations have been implemented at the University of Michigan. It also addresses violations of information use, and what consequences are applied by the University and courts of law to remedy those violations. Most importantly, it will help you understand your responsibilities as a user of institutional data.

## Using Information Correctly: Federal and State Acts

There are several important University, state, and federal policies that affect how we use information at the University of Michigan-Flint. These policies provide a framework within which we use, interpret, and distribute information. This section of the handout briefly summarizes the policies. The section entitled "Bibliography" contains information on how to obtain the complete version of each policy.

### *The Family Education Rights and Privacy Act*

The Federal Family Education Rights and Privacy Act (FERPA), also known as the "Buckley Amendment," directs The University of Michigan to keep certain student records private from third parties and to make others available for inspection and copying by students. Under the federal regulations implementing the act, every student in attendance at the University or who has been in attendance here has a right to inspect and review their "educational records." This includes a right to a response for explanations and interpretations of records and the right to obtain copies of the records.

### **Releasing Student Information**

The University may not disclose information from a student's record without first obtaining the written consent of the student; several exceptions are noted below. Parents of University students' 18-years or older do not have the right to have access to these records and are treated as any other member of the public unless the student has given written consent for release of such records to them.

Release without student consent may be done under certain limited circumstances. Some of the most common circumstances are:

- Release of public (directory) information regarding a current or former student. The University of Michigan-Flint has designated the following items as public information: name, home and local address and telephone, U-M school or college, class level, major field, dates of attendance at U-M, any degree received and date awarded, honors and awards received, participation in recognized activities, and previous school attended. However, a student has a right to refuse to have such information released. In such an event, the

student must file with the University's Registrar a request that such information not be released.

- The record may be disclosed to staff members who demonstrate a need to know consistent with their official functions for the University and consistent with normal professional and legal practices.
- The information may be released to state or federal educational authorities.
- The information may be used to determine the eligibility of the student for financial aid.
- The information may be released to organizations conducting studies for or on behalf of the University to develop, validate, or administer predictive tests, administer student aid programs, or improve instruction.

Questions regarding the disclosure of student educational records should be directed to the Office of the General Counsel.

**Note:** Information protected under FERPA is exempt from disclosure under the Freedom of Information Act (FOIA).

### *The State of Michigan Freedom of Information Act*

The State of Michigan Freedom of Information Act adopted on April 13, 1977, states that anyone is entitled to make a written request and obtain complete information regarding the affairs of government. Because the University of Michigan-Flint is a public institution, this act legislates that anyone may make a request to access, inspect, and make or obtain copies of any "writing" prepared, used, owned, possessed, or retained by any part of the University, except those records which are specifically exempt from inspection.

#### **Some types of information that are exempt from disclosure include:**

- "Information of a personal nature where the public disclosure of the information would constitute a clearly unwarranted invasion of an individual's privacy."
- "Information on or records subject to the attorney-client privilege."
- "Information or records subject to the physician-patient, psychologist-patient, minister, priest or Christian science practitioner, or other privilege recognized by statute or court rule."
- "Medical, counseling, or psychological facts or evaluations concerning an individual if the individual's identity would be revealed by a disclosure of those facts or evaluation."

## **Where can I go to get more information about FOIA?**

As responsible data users, you should be aware of your responsibilities as legislated by these acts. However, the interpretation of FOIA is a complex area of the law in which hundreds of court decisions need to be considered in order to develop a complete understanding of the principles governing disclosure of government information. The University has designated a Chief Freedom of Information Officer to handle requests under this act, including official denials. If you receive a request for a record that your department usually provides as public information, you can provide the record. However, if you are unsure of whether or not you should fulfill a request for information, contact the Chief Freedom of Information Officer's Office at (734) 763-5082.  
<http://www.umich.edu/~urel/foia.html>

### *The Federal Freedom of Information Act and the Federal Privacy Act of 1974*

Also to be considered are the Federal Freedom of Information Act and the Federal Privacy Act of 1974. These Acts are similar in substance to the State of Michigan FOIA, but pertain to federal records and data, such as social security numbers and information on federal grants and contracts. Both laws address the legitimate need to limit disclosure of particular information and need to be considered when determining if a request for information should be filled.

### *The Health Insurance Portability and Accountability Act of 1996 (HIPAA)*

The purpose of HIPAA is to ensure health insurance portability, reduce healthcare fraud and abuse, guarantee security and privacy of health information, and enforce standards for health information. In a nutshell, we must adequately protect all individually identifying health information from disclosure. HIPAA is extremely complicated. If you control or think you control records containing identifiable information about patients, be aware that you have strict obligations under HIPAA to protect those records as well as to inform patients about how you are using those records and to whom you are disclosing them. Contact the Office of the General Counsel's Health System Legal Office (734 764-2178) to get more specific assistance with how to manage health information under HIPAA.

## **Using Information Correctly: University Policy**

The University of Michigan has adopted several policies and guidelines on the proper use of information resources. These policies use FOIA and FERPA to establish the framework for data use.

## *Bylaw of the Board of Regents*

The Regents' Bylaw, section 14.07, states, "In collecting, utilizing, and releasing information about individuals associated with the University, the University will strive to protect individual privacy, to use information only for the purpose for which it was collected, and to inform individuals of the personal information about them that is being collected, used, or released. The University will not release sensitive information without the consent of the individual involved unless required to do so by law."

## *The Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan (SPG 601.7)*

The Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan policy regulates the use of all information technology resources at the University of Michigan. The policy:

- Supports access to information at the local, national, and international level.
- Supports an atmosphere of intellectual freedom and sharing of information.
- States that the "health and well-being" of the University information resources are the "responsibility of its users."
- Describes unethical and unacceptable behavior and lists disciplinary actions.
- Applies to the University community and all University information resources.
- Specifies disciplinary action up to and including dismissal for violations.

## *The Institutional Data Resource Management Policy (SPG 601.12)*

The goals of the Institutional Data Resource Management Policy are to:

- Manage information as a strategic asset to improve the quality of services to the student and the entire University community;
- Implement databases that are consistent, reliable, and accessible to meet all institutional requirements;
- Maximize the business processes through data management across business units.

This policy indicates that "The University of Michigan's institutional data resource, by definition, practice, and intent, is a University asset." As a recognized asset, the policy identifies that:

- The data resource will be safeguarded and protected.
- The data will be shared based on institutional policies.
- The data will be managed as an institutional resource.
- Institutional data will be identified and defined.
- Databases will be developed based on the needs of institutional processes.
- Information quality will be actively managed.

## *The Proper Use of Information Technology at the University of Michigan-Flint*

The Proper Use of Information Technology at the University of Michigan-Flint policy governs authorized, appropriate and responsible use of all information technology resources at the University of Michigan-Flint. The policy requires that all users:

- Respect the privacy of University records.
- Recognize the legal protection provided by copyright and license agreements for programs and data.
- Restrict activities to the intended use for which access to the resources was granted.
- Maintain the integrity of the computing systems.

## **Applying Policies to the Information Systems**

All the previously summarized policies apply to the information systems in use at the University of Michigan-Flint. In addition, this section identifies the steps you may take as a responsible data user to ensure the protection and appropriate use of data.

### *What Can You do to Secure the Data to which You have Access?*

ITS (Information Technology Services – UM-F) has a responsibility to provide a secure environment to protect centrally maintained data. As an individual, you have a responsibility to secure data in your local environment. Securing data means providing physical protection from unauthorized access. Some examples of measures you can take to secure data:

- Prior to sharing data with others, electronically or otherwise, ensure that the recipient is authorized to access the data and understands their responsibilities as a user.
- Turn off your desktop computer when not using it.
- Keep passwords to yourself.
- Lock confidential reports in a desk drawer when not using them.

## Information Misuse and Consequences

To clarify your responsibilities, this section provides examples of how data might be misused, unintentionally or deliberately.

### *Examples of Violations*

- Obtaining or attempting to obtain access to sensitive data not within the scope of one's University responsibilities.
- Using information for personal benefit, family, and friends.
- Releasing information in an inappropriate manner.
- Using information inaccurately, conflicting with published, sanctioned University information or statistics.

### *Consequences of Misuse*

The consequences of the misuse of information affect the University, individuals, groups, and violators. Here is a list of possible consequences to:

#### **The University**

- Loss of state and/or federal funding
- Lawsuits
- Loss of faith and trust on the part of employees and students

#### **Individuals or Groups**

- Violation of privacy
- Grievous bodily harm and/or mental duress
- Loss of opportunity or exclusion
- Discrimination

#### **The Violators**

- Disciplinary action administered by the supervisor in compliance with SPG 201.12 including fines, suspension, or dismissal
- Loss of credibility
- Lawsuit from the University or individuals/groups

# The Information Systems Access and Compliance Statement

**THE UNIVERSITY OF MICHIGAN-FLINT  
INFORMATION SYSTEMS ACCESS AND COMPLIANCE STATEMENT**

**PURPOSE:** By signing this form you certify that you have read the Access and Compliance document and that you agree to abide by the state and federal laws and University policies that apply to the proper use of data.

**RESPONSIBILITY:** The granting of access carries with it an implicit bond of trust that:

- You will be a responsible user of data, whether it is data relating to your own unit or another unit.
- Data that you obtain from these data sets will be stored under secure conditions.
- You will make every reasonable effort to maintain privacy of the data.
- You will make every reasonable effort to interpret the data accurately and in a professional manner.
- Prior to sharing data with others, electronically or otherwise, ensure that the recipient is authorized to access the data and understands their responsibilities as a user.
- You will sign off the systems when not using them.
- You will keep passwords to yourself.
- You will store/secure confidential and sensitive information, reports, etc in an appropriate manner when not using them.
- You will dispose of confidential reports in an appropriate manner when done with them.

**VIOLATIONS:** Misuse of the data in or from these data sets will subject you to disciplinary action as described in Standard Practice Guide section 201.12 (Discipline-Performance and Conduct Standards) and as deemed appropriate by executive authority.

**CERTIFICATION:** I have read the document entitled, *Access and Compliance; Proper use of University Information Systems*, and I understand my obligations as a responsible user of the data to which I have been granted access.

Name: \_\_\_\_\_ Uniqname \_\_\_\_\_

Signature: \_\_\_\_\_

Title: \_\_\_\_\_ Dept/Unit: \_\_\_\_\_

Campus Address: \_\_\_\_\_ Campus phone: \_\_\_\_\_

**SAMPLE FORM – PLEASE DO NOT USE**

**Completed forms should be sent to: ITS, 207 MSB**

## Bibliography

The following University publications and published policies may interest you if you want to further explore the topic of using Information Technology.

### *Available from Information Technology Services:*

- *UM-Flint Proper Use Policy*
- *Access and Compliance: Proper Use of University Information Systems*

### *Available from the Information Technology Division:*

- *In the Age of Information Technology, Think About It*
- *Using Software, A Guide to the Ethical and Legal Use of Software for Members of the Academic Community*
- *Proper Use Policy* <http://www.umich.edu/~policies>
- *Conditions of Use Statement*
- *Data Administration Guidelines for Institutional Data Resources*

### *Available from the University Audits Office*

- *University of Michigan Standard Practice Guide* <http://www.umich.edu/~spgonlin/>
  - Section 201.12 Performance and Conduct Standards
  - Section 601.5 Microcomputer Acquisition, Usage and Disposal
  - Section 601.7 Proper Use of Information Resources, Information Technology, and Networks at the University of Michigan. Performance and Conduct Standards
  - Section 601.12 The Institutional Data Resource Management Policy.

A number of policies within University units implement the broad policies described herein in more specific detail. In addition, higher education and computing industry publications frequently address the questions of security, access, ethics, and use of electronic information.