

DRAFT 7-14-2017
**REGENT POLICY DOCUMENT REVIEW:
RPD 25-3, “POLICY ON USE OF
INFORMATION TECHNOLOGY RESOURCES”**

BACKGROUND

The UW System Board of Regents’ policies are codified in Regent Policy Documents (RPDs) that have been adopted over time, some dating back to the creation of the UW System. The Board has adopted these policies under the authority granted in Chapter 36, Wis. Stats. The RPDs address a wide array of subjects, including academic policies and programs, contracts, student activities, and trust and investment policies.

Since 2011, the Office of the Board of Regents and UW System Administration have been working to review and update the RPDs. As part of this review process, the Board of Regents adopted a set of standards and protocols to direct the analysis of the RPDs. These standards include consideration of the extent to which a policy: addresses the UW System as a whole, establishing a fundamental principle as a basis and guide for later action; serves as an enduring statement rather than responding to a short term issue; addresses institutional risks, promotes operational efficiency, or enhances the missions of the UW System or UW institutions; and promotes compliance with applicable laws and regulations.

At its October 2017 meeting, the Business and Finance Committee will consider revisions to RPD 25-3, “Policy on Use of Information Technology Resources.”

REQUESTED ACTION

Adoption of Resolution I.2.x., which revises Regent Policy Document 25-3, “Policy on Use of Information Technology Resources” to be renamed “Acceptable Use of Information Technology Resources.”

DISCUSSION

In June of 1997, the Board of Regents adopted its policy regarding the use of information technology resources. Resolution 7461, now codified as RPD 25-3 (included as Attachment B), states that it is the policy of the UW System “to afford broad access to information technology resources for university students, faculty, and staff for use in fulfilling the university’s missions, and for appropriate university-related activities.” The current policy does not clearly define “information technology resources,” nor address what activities would be considered either acceptable or unacceptable use of information technology resources.

The proposed modifications to RPD 25-3 (Attachment A) provide a comprehensive description of what are considered “information technology resources.” The proposed changes also define acceptable uses of UW System information technology resources, and include a comprehensive and unambiguous description of what would be considered “unacceptable use.” The proposed policy retains aspects of the current policy that apply to privacy and other limitations on the use of information technology resources.

The proposed Board of Regents policy will be the sole policy for the System, and UW institutions will be required to post the policy on institutional websites.

RELATED LAWS AND REGENT POLICIES

Regent Policy Document 25-4, Strategic Planning and Large or High Risk Projects
Regent Policy Document 25-5, Information Technology: Information Security

DRAFT

Attachment A

Proposed Alternative to RPD 25-3 (6/19/2017)

Regent Policy Document 25-3 Acceptable Use of Information Technology Resources

Scope

This policy covers all those who access information technology (IT) resources under the control of the University of Wisconsin (UW) System.

Purpose

The purpose of this policy is to outline the expectations of the Board of Regents regarding the acceptable use of IT resources and to establish the parameters for the use of IT resources.

Policy Statement

IT resources are essential tools in accomplishing the mission of the UW System of disseminating and extending knowledge, fostering the free exchange of ideas, and providing effective support for teaching, research, and public service functions. It is the policy of the UW System Board of Regents that the use of and access to UW System IT resources is a privilege that extends to UW students, faculty, staff and other authorized users for use in fulfilling the university's mission, and for appropriate university-related activities.

UW System IT resources include all UW System equipment, facilities, technologies, and resources used for information processing, transfer, storage and communications. These include, but are not limited to, computer hardware and software, computer labs, classroom technologies such as computer-based instructional management systems, and computing and electronic communications devices and services, modems, email, networks, telephones, voicemail, facsimile transmissions, video, mobile computer devices, multimedia and instructional materials. This definition also includes services that are university owned, leased, operated, provided by the university or otherwise connected to university resources, such as cloud computing or any other connected/hosted service provided.

Acceptable and Unacceptable Uses of Information Technology Resources

Acceptable use of UW System IT resources includes any purpose related to the direct and indirect support of the System's educational, research, service, student and campus life activities; administrative and business purposes; financial systems; and human resources administration.

Authorized individuals, including currently-enrolled students, faculty, administrators, other employees, and other authorized users, are provided access to IT resources in order to support their studies, instruction, research, duties as employees, official business with the university, and other university-sanctioned activities according to their roles and responsibilities.

Employees, students, and other authorized users must not engage in unacceptable use of university IT resources, which includes but is not limited to the following:

1. Sharing or transferring to others authentication details, such as network IDs and passwords, or other access codes or circumventing user authentication which could allow unauthorized users to gain access to university IT resources;
2. Violation of federal, state, or local laws; institutional policies, rules or guidelines; or licensing agreements or contracts;
3. Harassment of, threats to or defamation of others; stalking; and/or illegal discrimination;
4. Storage, display, transmission, or intentional or solicited receipt of material that is or may reasonably be regarded as obscene, sexually explicit, or pornographic, except as such access relates to the academic or research pursuits of a student or employee;
5. Widespread dissemination of unauthorized email messages (e.g., mass mailings, spam, email chain letters); or
6. Damaging, disrupting or exposing IT resources to unauthorized access or harm.

In addition to the examples stated above, unacceptable use of university IT resources for UW System employees also includes the following:

7. Outside employment, commercial activities, or other forms of private financial gain;
8. Political lobbying, campaigning, or soliciting political contributions;
9. Wagering or betting;
10. More than minimal use for private or personal purposes that interferes with work or job performance or that interferes with the activities of other employees, students, or other authorized users.

Users must not use UW System information technology to speak on behalf of the UW System or use UW System trademarks or logos without authorization. Affiliation with the UW System does not, by itself, imply authorization to speak on behalf of the UW System. The UW System is not responsible for the content of documents, exchanges or messages, including links to other information locations on the internet that reflect only the personal ideas, comments, and opinions of individual members of the university community, even when this content is published or otherwise circulated to the public at large by means of UW System IT resources.

Privacy and Security

The UW System shall take reasonable measures to protect the privacy of its IT resources and accounts assigned to individuals. However, the UW System cannot guarantee absolute security and privacy. Users should be aware that any activity on UW System IT resources may be monitored, logged and reviewed by UW System-approved personnel or may be discovered in

legal proceedings. Generally, the contents of user accounts and personal communications will be treated as private and not examined or disclosed except:

- as required for system maintenance or business necessity, including security measures;
- when there exists reason to believe an individual is violating the law or UW System or institutional policy;
- to meet the requirements of the Wisconsin Public Records Law or other laws; regulations; or institutional policies, rules, or guidelines; or
- as permitted by applicable law or policy.

The UW System has the right to employ appropriate security measures, to investigate as needed, and to take necessary actions to protect university resources. The UW System may also have a duty to provide information relevant to ongoing investigations by law enforcement.

UW institutions will work with faculty, staff and students to protect their privacy interests, as well as those of the UW System.

Users must not violate the privacy of other users. Technical ability to access unauthorized resources or others' accounts does not by itself imply authorization to do so, and it is a violation of this policy to access others' accounts unless authorized to do so for a legitimate business purpose.

Other Limitations on Use of Information Technology Resources

In addition to the general principles set forth in this policy, the use of IT resources may be affected by other laws and policies; included among these are: federal copyright laws and privacy laws related to student records; state statutes related to computer crimes and political activities of state employees; ethical standards of conduct; dismissal for cause; standards and disciplinary processes related to academic and nonacademic misconduct by students; and conduct on university lands.

Failure to Comply with Information Technology Resource Policies

Failure to adhere to the provisions of this policy may result in the suspension or loss of access to UW System IT resources; appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff; civil action; or criminal prosecution. To preserve and protect the integrity of UW System IT resources, there may be circumstances where the university must immediately suspend or deny access to the resources.

Oversight, Roles, and Responsibilities

This policy constitutes the university's policy on the acceptable use of university IT resources. It applies systemwide and may not be replaced by, supplemented by or superseded by other policies. In order to assist members of the university community in fulfilling their

responsibilities with respect to use of IT resources, each University of Wisconsin institution shall post this policy on its website.

Related Regent Policies and Applicable Laws

- Family Educational Rights and Privacy Act (FERPA)
- Federal Copyright Law
- Chapter 11, Wisconsin State Statutes, Campaign Financing
- Chapter 19, Subchapter II, Wisconsin State Statutes, Public Records and Property
- Section 943.70, Wisconsin State Statutes, Computer crimes.
- Chapter UWS 4 Wisconsin Administrative Code, Procedures for Dismissal
- Chapter UWS 7 Wisconsin Administrative Code, Dismissal of Faculty in Special Cases
- Chapter UWS 8 Wisconsin Administrative Code, Unclassified Staff Code of Ethics
- Chapter UWS 11 Wisconsin Administrative Code, Dismissal of Academic Staff for Cause
- Chapter UWS 14 Wisconsin Administrative Code, Student Academic Disciplinary Procedures
- Chapter UWS 17 Wisconsin Administrative Code, Student Nonacademic Disciplinary Procedures
- Chapter UWS 18 Wisconsin Administrative Code, Conduct on University Lands
- Chapter UWS 21 Wisconsin Administrative Code, Use of University Facilities
- Regent Policy Document 20-22, Code of Ethics
- Regent Policy Document 21-4, Identity Theft Detection, Prevention, and Mitigation
- Regent Policy Document 25-4, Strategic Planning and Large or High-Risk Projects
- Regent Policy Document 25-5, Information Technology: Information Security

History: Res. 7461, adopted 06/06/1997, created Regent Policy Document 97-2; subsequently renumbered 25-3; Res. 10xxx, adopted xx/yy/zzz, amended Regent Policy Document 25-3.

Attachment B

CURRENT Regent Policy Document 25-3

Policy on Use of University Information Technology Resources

In accordance with its mission to disseminate and extend knowledge, to foster the free exchange of ideas, and to provide effective support for its teaching, research, and public service functions, it is the policy of the University of Wisconsin System to afford broad access to information technology resources¹ for university² students, faculty, and staff for use in fulfilling the university's missions, and for appropriate university-related activities.

Access by Individuals

Access to information technology resources carries with it the responsibility for ensuring that the use of these resources is primarily for university purposes and university-related activities, and for maintaining the integrity and security of the university's computing facilities. In the interest of making the use of information technology resources a natural part of the day-to-day work of all members of the university community, incidental personal use is tolerated. However, one should use non-university sources of e-mail, internet access, and other information technology services for activities of an extensive or recurring nature that are not related to university purposes. For the security of the information technology system, individuals having access to information technology resources must take reasonable care to ensure that unauthorized persons are not able to use their access to the system.

Dissemination of Information and Official Documents

Information technology resources are a dynamic mechanism for the free exchange of knowledge, and it is desirable for the university to foster the robust dialogue that results from the use of the resource, and to encourage students, faculty, and staff to participate in that dialogue. Those exchanges that reflect the ideas, comments, and opinions of individual members of the university community must, however, be distinguished from those that represent the official positions, programs and activities of the university. Students, faculty and staff using information technology resources for purposes of exchanging, publishing, or circulating official university documents³ must follow institutional requirements concerning appropriate content and style.

The university is not responsible for the content of documents, exchanges or messages, including links to other information locations on the internet or world wide web, that reflect only the personal ideas, comments, and opinions of individual members of the university

community, even where they are published or otherwise circulated to the public at large by means of university information technology resources.

Inter-institutional Cooperation

During times when they are away from the University of Wisconsin Institution where they are enrolled, students may benefit from the ability to use the information technology resources of another University of Wisconsin campus. To the extent possible with available resources, each University of Wisconsin System Institution should allow access to its information technology resources by students taking distance education and other courses from other University of Wisconsin System Institutions.

Limitations on the Availability of Information Technology Resources

The university's information technology resources are, by nature, finite. All members of the university community must recognize that certain uses of university information technology resources may be limited for reasons related to the capacity or security of the university's information technology systems, or as required for fulfilling the university's primary teaching, research, and public service missions.

Privacy and Confidentiality of Electronic Documents

No information technology resources can absolutely guarantee the privacy or confidentiality of electronic documents. University of Wisconsin Institutions should, however, take reasonable precautions to protect electronic documents containing private and confidential information, and to assure persons using university information technology resources to transmit e-mail or electronic documents that the university will not seek access to their messages or documents except where necessary to:

1. Meet the requirements of the Wisconsin Public Records Law, or other statutes, laws, or regulations ;
2. Protect the integrity of the university's information technology resources, and the rights and other property of the university;
3. Allow system administrators to perform routine maintenance and operations, and respond to emergency situations; or
4. Protect the rights of individuals working in collaborative situations where information and files are shared.

University of Wisconsin System Institutions may choose to establish more detailed procedures for determining when access to electronic documents will be sought by the institution. As encryption products become more readily available, institutions may also wish to make them available to information technology users as appropriate to protect privacy interests.

Other Limitations on Use of Information Technology Resources

In addition to the general principles set forth in this policy, the use of information technology resources may be affected by a number of other legal and ethical principles. While it is not possible to list all potentially applicable laws and regulations, the following are particularly likely to have implications for the use of university information technology resources:

1. Ethical standards of conduct for the appropriate use of one's university position and university resources are established for faculty and academic staff in Chapter UWS 8, Wisconsin Administrative Code, and for classified staff in Chapter ER-MRS 24, Wisconsin Administrative Code.
2. Chapters UWS 14 and 17, Wisconsin Administrative Code, establish standards and disciplinary processes relating to academic and nonacademic misconduct by students, including prohibitions on disruption of university activities, damage to university facilities, harassment, and similar matters.
3. Chapter UWS 18, Wisconsin Administrative Code, governs conduct on university lands, and applies to all members of the university community. Chapter UWS 21, Wisconsin Administrative Code, regulates the use of university facilities.
4. Section 943.70, Wisconsin Statutes, defines and prohibits certain computer crimes.
5. Chapter 11, Wisconsin Statutes, restricts the use of state facilities for political activities by state employees.
6. The federal copyright law applies to materials published or circulated through the use of computing resources.
7. The federal Family Educational Rights and Privacy Act restricts access to personally identifiable information from students' education records. Students, faculty and staff are responsible for understanding and observing these and all other applicable policies, regulations and laws in connection with their use of the university's information technology resources.

University of Wisconsin System Institution Responsibilities

In order to assist members of the university community in fulfilling their responsibilities with respect to use of information technology resources, each University of Wisconsin Institution shall disseminate this policy, together with guidance, as to any specific campus policies affecting the use of information technology resources.

Failure to Comply with Information Technology Resource Policies

Failure to adhere to the provisions of this policy may result in the suspension or loss of access to university information technology resources, appropriate disciplinary action as provided under existing procedures applicable to students, faculty, and staff, or civil or criminal prosecution.

To preserve and protect the integrity of information technology resources, there may be circumstances where the university must immediately suspend or deny access to the resources. Should a student's access be suspended under these circumstances, the university shall inform the student immediately and shall afford the student an opportunity to respond.. The university shall then determine whether disciplinary action under Chapter UWS 17, Wisconsin Administrative Code, or some alternative course of action, is warranted and shall follow the procedures established for such cases.

1 Information technology resources include computers, software, e-mail accounts, internet access, and similar computing tools.

2 "University" is used in this document to refer to the University of Wisconsin System and its institutions.

3 Official university documents are those which purport to speak for the university and its official programs and departments, such as policy documents, official forms, curriculum information, institutional statistics, and departmental home pages on the world-wide web.

4 The electronic records of university employees are subject to disclosure in accordance with the Wisconsin Public Records Law. Student records, including electronic documents, are protected against disclosure by the Family and Educational Rights and Privacy Act, which restricts access to personally identifiable information from students' education records.

History: Res. 7461 adopted 6/6/97.
