

Acceptable Use Policy for UWM

Spring 2005

Final Version as of: April 12, 2005

**Guidelines for Appropriate Use of University of Wisconsin-Milwaukee Information
Technology Resources**

1. UWM provides access to computers, databases, electronic mail, the Internet, software, and other University information technology (IT) resources to its faculty, staff and students, as well as community members, in order to facilitate the pursuit of excellence in the University's missions of scholarship, learning, teaching, research, and service.

2. In order to preserve access to University IT Resources for the entire community, everyone is expected to know and adhere to the appropriate University, state and federal regulations and guidelines.

3. In addition to this policy, the regulations that govern personal conduct and use of University facilities also apply to the use of IT resources.

4. **General Guidelines**
University IT Resources are owned by UWM. Access to them is a privilege granted to members of the University community and carries with it the responsibility to use them for University related activities, while exercising common sense and civility.

5. **Individual Responsibility**
Authorization for use of IT facilities is provided to each individual for his or her own use. No one may use an authorization that belongs to someone else. Everyone is expected to protect the confidentiality of their personal identification codes and passwords. Everyone is expected to realize that in many cases the University has obtained access to IT resources exclusively for the use of members of the University community.

6. **Security**
Protection of the University IT resources depends upon everyone taking reasonable care to insure that unauthorized persons are not able to use their identification codes, passwords or privileges.

7. **Misrepresentation**
Persons may not misrepresent themselves when accessing University IT resources or when using those resources for any form of electronic communication. Persons may not obtain or use – or attempt to obtain or use - passwords or other access credentials that have not been either assigned to them as individuals, or provided for their use as University employees.

8. **Malicious activity**
Persons may not alter or intentionally or unreasonably damage, disrupt, impair or waste University IT Resources or interfere with another person's authorized access to them.

9. Commercial, Political and Non-University Activities

Persons may not use University IT resources to promote or solicit sales for any goods, services, unauthorized charities, or other contributions unless such use conforms to UWM rules and regulations governing the use of University resources or unless such efforts are on behalf of a student organization recognized by the University. University employees may not use University IT Resources to solicit donations for a political campaign external to UWM. Except for research collaborations, no one may use University IT Resources to promote or advance the interests of any for-profit non-University entity, group or organization for commercial purposes unless appropriately authorized.

10. Incidental Personal Use

In the interest of making the use of University IT Resources a natural part of the day-to-day work of all members of the University community, incidental personal use is accepted. Nevertheless, 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 do not serve University purposes.

11. Violations of other laws

Persons may not use University IT resources in a manner that violates federal, state, UW System or University of Wisconsin–Milwaukee policies, regulations or laws.

12. Use of Commercial Software

All persons using University-provided software must do so only in accord with the applicable license agreement. Persons may use personally owned software on University owned computers provided there is no adverse impact on University IT resources and documentation of software ownership is kept and available at the site where the computer is normally located.

13. Development of Software

Ownership and intellectual property rights for software developed by University employees in various circumstances are outlined in UW System Financial and Administrative policy G10.

14. Sanctions

Violation of University rules governing appropriate use of IT resources may result in loss of access privileges, University disciplinary action, and/or criminal prosecution. The appropriate due process and policies will be followed depending upon whether faculty, academic staff, classified staff or students are alleged to be involved.

15. Administrative Access to IT Resources

Although the University respects a diversity of perspectives and accordingly does not condone either censorship or the unauthorized inspection of electronic files, persons should be aware that the normal operation and maintenance of University IT resources require the backup of data and records, the logging of activity and the monitoring of general usage patterns. IT staff members must respect and ensure the confidentiality and privacy of the data they observe or access during the course of performing their duties.

16. Monitoring/Disclosure of Files or Activity

Consistent with the constraints of confidentiality, the University may inspect files stored on any University IT resources or monitor usage when there is cause to believe that a law or a UW System or UWM policy has been violated, when there is need to defend a civil or criminal claim filed against the University, or in conjunction with a workplace misconduct investigation. Each person should be aware that their electronic records, files and communications may be subject to the University's obligation to respond to subpoenas or other court orders, reasonable discovery requests, internal audits and requests for documents pursuant to the Wisconsin Public Records Law. The appropriate due process and policies will be followed depending upon whether faculty, academic staff, classified staff or students are alleged to be involved.

17. Unit IT policies

Individual units within the University may have supplemental written guidelines for use of those University IT resources that are under their control. Such guidelines must be consistent with this policy, but may provide additional detail, restrictions, and user guidelines. Such policies must be disclosed to those who are potentially affected by them.

APPENDIX – Laws and Policies

- Section 17 U.S.C §101, et al., which is federal copyright law (<http://www4.law.cornell.edu/uscode/17/101.html>)
 - Section 18 U.S.C. 1030, the federal law regarding fraud and related activity in connection with computers (<http://www4.law.cornell.edu/uscode/18/1030.html>)
 - Section 20 U.S.C. § 1232g, the Family Educational Rights and Privacy Act (FERPA) (<http://www4.law.cornell.edu/uscode/20/1232g.html>)
 - Section 18 U.S.C. § 1462, the federal law concerning importation or transportation of obscene matters (<http://www4.law.cornell.edu/uscode/18/1462.html>)
 - Section 18 U.S.C. § 1465, the federal law regarding transportation of obscene matters for sale or distribution (<http://www4.law.cornell.edu/uscode/18/1465.html>)
 - Chapter 11, Wis. Stats., which restricts the use of state facilities for political activities by state employees (<http://www.legis.state.wi.us/statutes/Stat0011.pdf>)
 - Section 943.70, Wis. Stats., which defines and prohibits certain computer crimes (<http://www.legis.state.wi.us/statutes/Stat0943.pdf>)
 - Section 948.12, Wis. Stats., which prohibits possession of child pornography (<http://www.legis.state.wi.us/statutes/Stat0948.pdf>)
 - Chapter UWS 8, Wis. Admin. Code (for faculty and academic staff) and Chapter ER-MRS 24, Wis. Admin. Code (for classified staff), which explain ethical standards of conduct appropriate for use of one's University position and University resources (<http://www.legis.state.wi.us/rsb/code/uws/uws008.pdf> and <http://www.legis.state.wi.us/rsb/code/er-mrs/er-mrs024.pdf>)
- Chapters 6 (for faculty) & 13 (for academic staff), Wis. Admin. Code, which explain complaints and grievances processes
<http://www.legis.state.wi.us/rsb/code/uws/uws006.pdf>
<http://www.legis.state.wi.us/rsb/code/uws/uws013.pdf>
- Chapters UWS 14 and 17, Wis. Admin. Code, which 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 (<http://www.legis.state.wi.us/rsb/code/uws/uws014.pdf> and <http://www.legis.state.wi.us/rsb/code/uws/uws017.pdf>)

- Chapter UWS 18, Wis. Admin. Code, which governs conduct on University lands (<http://www.legis.state.wi.us/rsb/code/uws/uws018.pdf>)
- Chapter UWS 21, and UWM's Use of Facilities Policy (Selected Academic and Administrative Policy S-23), which regulate use of University facilities (<http://www.legis.state.wi.us/rsb/code/uws/uws021.pdf> and http://www.uwm.edu/Dept/SecU/acad+admin_policies/S23.pdf)
- UW System Regent Policy Document 97-2, "Policy on Use of University Information Technology Resources" (http://www.uwsa.edu/bor/rpd/bor_pols.pdf)
- GAPP 10 of the UW System, Computer Software Ownership, (<http://www.uwsa.edu/fadmin/gapp/gapp10.htm>)
- UWM Equal Employment Opportunity Policy (http://www.uwm.edu/Dept/OD_C/policies.html#eeop)
- UWM Discriminatory Conduct Enforcement Procedures (http://www.uwm.edu/Dept/SecU/acad+admin_policies/S47.pdf)
- The UWM FERPA Manual (<http://www.des.uwm.edu/intranet/ferpa/ferpamanual.pdf>)
- Laws and Policies Ensuring the Confidentiality of Human Research Subjects, including the Health Insurance Portability and Accountability Act (HIPAA) and associated regulations and the UWM Guide to Human Subjects Research Protocols (<http://www.hhs.gov/ocr/hipaa/> and <http://www.uwm.edu/Dept/RSA/Public/IRB/Guide/index.html>)