Policy on the Use of Computing Resources

Augsburg's Information Technology organization advances the mission of the University by providing an online framework for our vibrant, modern learning community. Much like city planners who organize the resources of a physical community, Information Technology (IT) works closely with the university community to plan, build and support an online framework for Augsburg upon which we communicate, enroll, learn, teach, research, and manage.

A. It is the policy of Augsburg University that computing resources be used in a legal, ethical and responsible manner.

B. Any use of computing resources that would impede teaching, learning, research or administration; or that would violate an applicable license or contract is a violation of this policy.

Violation of this policy may result in immediate suspension of computing privileges, with referral to appropriate University or criminal authorities for consideration of penalties which may include dismissal or other discipline. This document is intended to work in conjunction with existing policies within the Augsburg University Student Guide, the Student Handbook, the Augsburg University Faculty Handbook, the Augsburg University Employee Handbook, and the departmental technical policies and standards as administered by Information Technology.

The University maintains **Computing Resources Usage Guidelines** to help you understand and comply with this policy. Any questions regarding interpretation or application of this policy should be directed to the Chief Information Officer.

Computing Resources Usage Guidelines

Although most people use computing resources in a legal, ethical and responsible manner, it is possible that willful or even accidental misuse can seriously disrupt the work of others. These guidelines are provided to increase your awareness of the issues involved.

1. University Use
Augsburg University computing resources are for use only by those persons with valid accounts or with the permission of the University to use computing resources.

2. Account Use
All accounts have a password to prevent unauthorized access of the account. You should not share your password with anyone or write it down in a publicly viewable location, as you are responsible for activity associated with your account. Passwords should be changed periodically to keep the account secure.

3. Unauthorized Access and Impersonation
Users may not attempt to gain access to computer systems, files, messages, communications, or documents of others unless they have a legitimate reason to do so. Accessing systems, files, messages, communications, or documents of others without a legitimate reason is inappropriate and is prohibited. Users may not impersonate other users or forge communications such as electronic mail messages.

4. Harassment
The University's policies prohibiting all forms of precluded discrimination, including sexual harassment, cover all forms and means, including those activities using computing resources. Computing usage that is perceived by another as discriminatory or sexually harassing as defined by the University policy may be considered a violation.

The display of offensive material in any publicly accessible area is likely to violate the University harassment policy. There are materials available on the Internet and elsewhere that some members of the University community will find offensive. Sexually explicit graphics is one example of such material. While the University cannot restrict the availability of such material, it considers their public display to be unethical. This includes, but is not limited to, output of such material to publicly accessible computer screens and printers.

5. Maliciousness
Computing resource users may not deliberately disrupt the performance of computer systems or networks, or attempt to circumvent system security. This includes reconfiguring a computer system to make it unusable for others, attempting to destroy or alter data or programs belonging to other users.

6. Commercial Activity
The use of University computing resources for commercial purposes or for personal gain is prohibited.

7. Sensitive Information
Users who have access to or store sensitive information belonging to the University on their computers must take extra precautions to keep this information secure. The use of file sharing software can inadvertently expose all of the data on a computer to public view. Employees who deal with sensitive data belonging to the University should store it in the appropriate network storage space where access rights are controlled.

8. Copyright
Distributing copyrighted material without approval of the copyright holder is illegal.

Revision History

Revision	Change	Date
1.0	Original Version	1999
1.1	Revision history section added	5/25/2009
1.2	Revised Community Definition	3/1/2011
1.3	Removed broken link to harassment policy	4/15/2011
1.4	Updated departmental mission statement and changed College to University	3/23/2018