Century Community and Technical College
5.22.0.1 Acceptable Use of Information Technology Resources

Purpose

The purpose of this policy is to establish written guidelines for the appropriate use of information technology resources at Century College.

Definitions of Terms Used in this Document

Information technology (IT): any computer; telephony equipment; network equipment; peripheral; storage device; data file

Community: any MnSCU employee, student, alumnus, authorized guest, and vendor

User: any person using any IT equipment or service, either locally or remotely

Provision of Services

Century College provides IT resources in support of its mission to continuously improve student understanding and capabilities that lead to purposeful lives, contribute to a vital community and pursue lifelong learning. As an institution of higher education, the College intends to provide the community with open and unrestricted avenues of communication as long as such use is in compliance with state and federal laws, other Century College policies, and MnSCU policies. The College reserves the right to summarily limit or suspend access to facilities, equipment, and services, as necessary, to comply with applicable laws, to protect the interests of Century College and other members of the community, and to preserve the integrity and performance of IT systems.

As with all IT services, local and long distance telephone services are provided for employees to conduct college-related business. Employees should limit their use of the telephone for personal communications. Any employee wishing to make a personal long distance call must use a pay phone, a personal phone card, a collect call, or have the charges applied to their home number. IT staff routinely review the log of long distance calls charged to the college and will request that employees reimburse the college for all calls not directly related to college business.

Priority of Use

While the College does not strictly limit the use of information technology services, activities related to the College's educational mission take precedence. Use of IT resources for personal or recreational activities may be limited depending on the capacity of the IT systems to support such activities.

Rights and Obligations

All users are responsible for using Century College IT resources in an appropriate manner. All applicable laws, statutes and policies related to personal behavior apply to electronic communications. Such laws and policies prohibit, among other things, lewd or indecent conduct, threat of physical harm, stalking, forgery, disruption of College services, damaging or destroying of property, discrimination and sexual harassment. All users are expected to respect the integrity of all security controls and abide by all security measures that have been implemented, as well as adhere to all end-user license and contractual agreements associated with Century College IT resources.

Cooperation with Investigations

Depending on the nature and severity of an alleged violation, Century College may notify the appropriate campus or external authorities for further investigation and possible disciplinary action or prosecution. Users violating Century College policies or state and federal laws may be subject to prosecution. While Century College technical staff members strive to provide reliable and secure IT resources, users should not consider the data storage or transmission systems to be secure and/or private.

Any data stored or transmitted using Century College IT resources may be considered to be Century College property and is subject to examination by supervisors or law enforcement under circumstances warranting investigation. Under these circumstances, access to any files stored using Century College IT resources will be provided to supervisors, or any other college administrators in the direct line of reporting, upon request.

Enforcement

Century College may deny members of the community who violate this policy or otherwise use Century College IT resources to violate other established policies or laws access to IT resources. Violations that constitute a breach of the Student Conduct Code or other Century College policy may be referred to the respective campus authority for review and possible disciplinary action.

Reporting and Notification

If a potential violation occurs in a college classroom or lab, violations should be reported to the faculty or staff monitoring the facility, or to the Director of Information Technology. If a potential violation occurs in a non-instructional area, the situation should be reported to the supervisor of the area.

Where appropriate, whoever is notified first shall review the activities and, if merited, notify the user that they are in violation of this policy and request that they take immediate remedial action to bring their conduct into compliance. The violation should then be reported to the Director of Information Technology as soon as possible so damage to data or system integrity may be assessed. College personnel may take immediate action, as needed, to abate ongoing interference with network and system operations, or to insure system integrity.

Complaints or Grievances

If a user’s access to IT resources is suspended as a result of an investigation, the alleged violator may appeal the suspension to the Director of Information Technology, then to the appropriate Vice President, and finally to the President, in that order.

If an allegation relates to personal harassment or similar behavior, the staff or administrator will direct the affected person to file a complaint with the responsible authority using established procedures. Staff and administrators will cooperate fully in investigations, but should not file complaints on behalf of aggrieved parties. The decision to file a complaint or prosecute is the responsibility of the affected party.

References

Minnesota State Colleges and Universities Board Policy 5.22 Computer Usage Policy

Date Proposed:	1/96
Date Approved:	3/96
Date Implemented:	3/96
Date Revised:	4/97 6/98 10/11/00 (renumbered) 2/01/01

Principles of Responsible IT Use

The following principles and examples are intended to illustrate some examples of unacceptable actions rather than to exhaustively list every specific behavior that may violate the Acceptable Use Policy. These principles are derived directly from the same standards of common sense and decency that apply to the use of any public resource.

Principle #1: Respect the privacy and rights of others.

Users may not use any Century College IT resource to:

- attempt to gain unauthorized access to any system, network, service, or data inside or external to Century College;
- monitor network traffic or undertake comparable measures without specific permission from the Director of Information Technology;
- store or run programs that are designed to capture keystrokes, passwords, mouse clicks, or data;
- send e-mail that is intended to intimidate or harass;
- create a hostile working or learning environment by displaying sexually explicit images or sounds;
- violate any laws pertaining to child pornography, obscenity, and defamation;
- duplicate or install software except in strict accordance with applicable licensing agreements and with permission from the Director of Information Technology;
- house or distribute unauthorized software, music, video or other information resources.

Principle #2: Respect other people's ability to benefit.

Users may not use any Century College IT resource to:

- engage in activities which compromise institutional systems or network performance;
- interfere with the institution's ability to provide the best possible service to the overall community;
- run programs that introduce a virus, worm or another destructive or disruptive program;
- launch "denial-of-service" attacks against internal or external systems;
- create, transmit or forward electronic chain letters, spam, or mail bombs.

Principle #3: Identify yourself truthfully.

Users may not use Century College IT resources to:

- falsely identify themselves in communications;
- attempt to "spoof" or otherwise represent their network activities as originating from a network address other than the actual source.

Principle #4: Unauthorized commercial use is prohibited.

Users may not use Century College IT resources to:

- conduct commercial activities without prior written authorization from the President;
- market a home business;

- host a commercial web page;
- allow anyone who does not have authorized use to access any IT resource or service;
- conduct political campaigns;
- operate unauthorized information services.