

North Hennepin Community College

Policy/Procedure Information

Number: 5.22.1

Name: Acceptable Use of Computers and Information Technology Resources Procedure

Author: Chief Information Officer

Custodian: Policy Committee

Effective Date: January 14, 2013

Next Review Date: AY2016 – 2017

Regulatory Authority:

- MnSCU Board Policy 5.22, [Acceptable Use of Computers and Information Technology Resources](#)
 - MN Statute 43.A38, [Code of Ethics for Employees in the Executive Branch](#)
-

Part 1. Purpose

This procedure establishes acceptable use procedures of NHCC information technology resources by students, employees, outside vendors and other community members, including the general public. Technology resources are the property of Minnesota State Colleges and Universities and use of said properties is a privilege based on compliance with Policy 5.22.

Nothing in this procedure shall be interpreted to expand, diminish or alter academic freedom.

Part 2. User Responsibilities

The goal of the NHCC Academic and Technology Services is to provide computer users with state of the art computing facilities and classrooms and to keep the number of restrictions on the individual to a minimum, while maintaining excellent service for students pursuing their academic goals and for employees conducting their work activities. To assist the College in achieving these objectives, users themselves must observe reasonable standards of behavior in the use of these facilities. A user of NHCC information technology resources shall abide by the following:

1. Obtain necessary accounts and passwords and be responsible for maintaining the security of all those accounts on NHCC's information technology systems.
2. Users may not authorize anyone to use any of their accounts for any reason. Users are responsible for all usage of their accounts. Users must take all reasonable precautions, including password maintenance and file protection measures, to prevent use of their accounts by unauthorized users. Users are not to provide others with access to any NHCC information technology resources.
3. Users may not impersonate or misrepresent another user's computer account or email user name.

4. Files owned by individual users are to be considered as private, whether or not they are accessible by other users. The accessing or attempting to gain unauthorized access into any account to use, read, transfer, copy or change contents in any way of another user's account will be viewed as theft of NHCC resources and as computer fraud.
5. Because many of the technological resources of NHCC are shared, the use of such resources for endeavors not directly related to enhancing and facilitating instruction and scholarly research activities will be considered secondary activities. Should such secondary activities interfere in any way with the primary activities of instruction and research, they may be terminated immediately.
6. Access to NHCC computer resources must not be abused either by attempting to harm the systems or by stealing copyrighted/licensed software or by installing unlicensed software. Software may not be installed on campus computers unless NHCC is the authorized owner and permission is granted by the Academic and Technology Services department. Federal Copyright Laws must not be violated by downloading copyrighted audio, video, graphics, or text materials from the internet without proof of proper licensing arrangements. Attempting to gain unauthorized access to any information technology resource or alteration of system hardware or software configurations is prohibited. Open-source software may be authenticated at the time of download by the authorized Academic and Technology Services administrator.
7. Information technology resources are not to be used for profit or commercial activity of any kind or for solicitations on behalf of groups, organizations, etc. that are not related to NHCC.
8. NHCC's information technology resources will not be used to violate any NHCC policies; city, state, or federal laws; or contracts and agreements entered into by NHCC.
9. No unauthorized attempt will be made to connect to and/or gain access to information being transported by computer networks, or to install, run or place software designed for this purpose on any College computer. Installation or use of any network communication software or device in order to steal information or identities is prohibited.
10. Only NHCC-owned technology, telephony and wireless technology systems will be configured and implemented on the NHCC network by NHCC Technology Services staff. NHCC-user bring-your-own device (BYOD) that meets NHCC BYOD requirements must be authorized and approved prior to the NHCC-user performing self-service installation and support including cable and peripheral connections.
11. Non-portable computer equipment is not to be removed from NHCC campus without written loan authorization between the NHCC Academic and Technology Services department, NHCC user, and NHCC user's Dean and/or Director.
12. Accidental damage, or damage caused by other parties, should be reported as soon as possible so that corrective action may be taken.
13. Using computing resources to interfere with the normal operation of college computing systems and connected networks including, but not limited to, introducing viruses, flooding the network with messages, sending chain letters, downloading or transferring excessively large files, or unfairly monopolizing resources that results in the exclusion of others in such a way that it causes disruption in instruction, computer labs or exploits network security and/or other vulnerabilities is prohibited. Intentionally causing any damage to any equipment is prohibited.
14. Harassment, threats to or defamation of others, stalking, and/or illegal discrimination is prohibited
15. Storage, display, transmission, or intentional or solicited receipt of material that is or may be reasonably regarded as obscene, sexually explicit, or pornographic is prohibited, including any depiction, photograph, audio recording, video or written word, except as such access relates to the academic pursuits of a system student or professional activities of a system employee. Individuals may be asked to desist and Public Safety may be called.
16. If a user identifies a potential security problem with an employee, the problem should be reported to the Dean of Academic and Technology Services immediately and should not be discussed with any other party.

17. NHCC does not employ filtering software or content blocking of any material found on the Internet on most of its computers. Parents and legal guardians should be aware that during the course of Internet use, patrons (including minors) may encounter material which could be considered objectionable or offensive. Parents and legal guardians are solely responsible for educating and monitoring the activity of a minor in their legal custody and are responsible for all activity that a minor takes during use of computing resources. Additionally, all applicable policies related to use of NHCC resources by a minor do apply.
18. As the information technology environment and laws change, the General User Policies and Procedures may be modified or amended through the NHCC Policy process at any time. Notice of any such modifications shall be provided by email to users. Users are responsible for keeping informed of the current policies. Questions about these policies should be directed to the Dean of Academic and Technology Services department.

Part 3. Enforcement

The above is a representative set of rules and guidelines. Any individual whose conduct violates the above guidelines or is not consistent with what is expected of a competent computer user will be subject to the following actions:

1. The account will be immediately deactivated.
2. The appropriate administrative authorities (NHCC, state, or federal) will be informed.
3. The appropriate administrative authorities will act. Actions taken by the administrative authorities will depend on the severity of the computer abuse. The NHCC Code of Student Conduct, bargaining unit contracts, the Academic Policies and Procedures Manual, and state and federal laws, will be used in determining appropriate sanctions.

| Review Action | Date(s) |
|----------------------------------|--|
| Campus Community Review Period | October 29, 2012 – November 12, 2012 |
| Shared Governance Council Review | November 30, 2012 |
| Labor/Management Meetings Review | MMA: November 27, 2012 MAPE: November 28, 2012 AFSCME: November 28, 2012 |
| Student Senate Review | November 27, 2012 |
| President Approval | December 3, 2012 |
| Campus Community Dissemination | December 7, 2012 |

History

- Originally adopted, May 29, 1996
- Replaced by MnSCU policy, May 12, 2004
- Revised December 2012
 - Procedure number changed from V.01 to 5.22.1
 - Changed Information Technology to Academic and Technology Services
 - Added language referring to a BYOD procedure
 - Modified language regarding harassment

- Modified language regarding obscene, sexually explicit, or pornographic material