Herkimer County Community College

Information Technology Department

Acceptable Use Policy (AUP) and Procedures

Version 3.13

Revised: September 18, 2019

Table of Contents

Purpose:

The purpose of this policy is to outline the acceptable use of information technology resources at Herkimer College. The scope of this policy contains, but is not limited to any equipment, accessories, software, networks, and electronic data that belongs to the College. This policy is intended to reflect the College's commitment to serve our learners by providing high quality, accessible educational opportunities and services described in the mission and core values statement.

General Information:

Technology resources are provided to members of the Herkimer College community for use in their prescribed tasks as well as for personal and professional development. In order to have access to technology resources, the Herkimer College Computer Use Policy must be read and acknowledged in Student Online Services (hereinafter referred to as SOS). The Information Technology Department provides user accounts as appropriate. Use of these resources is a privilege, not a right, and access is granted with restrictions and responsibilities for their use.

Technology abuse is costly and can have far-reaching negative consequences from disrupting the educational process to financial loss and/or reputation damage. Certain misuse of Herkimer College technology resources can result in revocation of technology privileges, suspension, dismissal and/or criminal prosecution.

Herkimer College values diversity of values and perspectives, and thus the College is respectful of the freedom of expression. However, Herkimer College reserves the right to restrict the use of technology resources in appropriate circumstances in which there may be violations of College policies, State or Federal laws. The College reserves the right to determine the appropriateness of the restriction, which includes but is not limited to removal of any material.

Rights and Responsibilities:

The Herkimer College network can provide access to resources on and off campus, as well as the ability to communicate with other users. Such access is a privilege and requires that individual users act responsibly. Users must respect the rights of others, the integrity of information systems and related physical resources, and follow all relevant laws, regulations and contractual obligations.

Students and employees may have rights of access to information about themselves stored in information systems, as specified in federal and state laws. Files may be subject to search under court order. In addition, system administrators may access user files and email as needed to protect the integrity of information systems. For example, following organizational guidelines, system administrators may access or examine files, emails or accounts that are suspected of unauthorized use/misuse or that have been corrupted or damaged.

Existing Legal Context:

All existing laws (federal and state), campus regulations and policies apply, including not only those laws and regulations that are specific to computers and networks but also those that may generally apply to personal conduct.

Misuse of technology resources may result in the restriction of computing privileges. Additionally, misuse can be prosecuted under applicable statutes. Users may be held accountable for their conduct under any applicable campus policies, procedures, or collective bargaining agreements. Complaints alleging misuse of campus technology resources will be directed to those responsible for taking appropriate disciplinary action under due process. Reproduction or distribution of copyrighted works, including, but not limited to, images, text, or software, without permission of the owner is an infringement of U.S. Copyright Law and is subject to civil damages and criminal penalties including fines and imprisonment. Notwithstanding, certain uses of material in an educational setting may be allowed under Fair Use. Questions about whether specific uses are permitted or not should be referred to the Director of Library Services.

General Access and Use of Computer Labs:

The academic computing labs are available to the following individuals for use in conjunction with coursework and other legitimate non-commercial educational purposes:

- Currently enrolled students of Herkimer College
- Current faculty and staff members of Herkimer College

The following group is admitted to academic computer labs on a space available basis, upon presentation of appropriate identification:

- Teachers and other professional employees of school districts and other public agencies that have been granted guest accounts on Herkimer College equipment.

Use of computer equipment is subject to the directives given by the person in charge of the lab (faculty, staff member, technician, student work-study) and by Campus Safety personnel.

The following rules govern the general use of the computer labs and equipment by students:

- No food, drink, smoking or mobile devices use is allowed in any computer lab.
- With respect to your peers, keep the noise level to a minimum while in the lab.
- Children are not allowed in any computer lab unless part of a formal college activity designed for children.
- Labs are not available during an instructional class.

- The person on duty may request a valid Herkimer College ID at any given time while working on a computer in an open lab.
- Students are expected to be polite and courteous to all personnel on duty at the time.
- Students should make sure they save all their work in their network account, i.e., My Documents Folder on your M:\ drive, not on the C:\ drive. Save your work frequently; every 15 minutes is recommended.
- Never leave any computer while you are logged into your account. If you must leave, please save your work, close all applications and log off the computer.
- If students are having problems with a computer or printer, they must ask the person on duty for assistance or call the Help Desk at 8555. Students must not attempt to fix the problem.
- If students are having trouble with class assignments, they should ask their instructor for help or contact the Academic Support Center (hereinafter referred to as ASC) for further assistance. Technicians and work-study staff are not required to help students with assignments and students should not ask them.

Unacceptable and Unauthorized Use:

Unacceptable and unauthorized activities can result in revocation of computing privileges, further disciplinary action, and filing of civil and/or criminal complaints. Herkimer College will cooperate with law enforcement authorities in investigations involving illegal activities for which college-owned computer and network resources are employed.

The technology resources may not be used for the following:

- For access to an account or system, you are not authorized to use.
- For any purpose contrary to the College's best interests.
- For deliberately wasting information technology resources such as, but not limited to overloading computing and printing resources, and intentionally wasting network bandwidth.
- For violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by Herkimer College.
- For projects resulting in financial gain unrelated to an individual's College duties.
- For the conduct of private business affairs in conjunction with programs that are designed to probe, describe, or to defeat computer security features of information

systems located at Herkimer College or elsewhere, or the repeated use of ordinary tools in a manner that may probe or describe network topology or computer security features without the express written consent of the Director of Information Technology or designee.

- For the introduction of malicious programs into the network or servers, including but not limited to the following: viruses, worms, trojan horses, spoofing, email spamming, crypto mining.
- For effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the user is not an intended recipient or accessing any information systems that the user is not expressly authorized to access unless these duties are within the scope of regular duties. This includes, but is not limited to, any types of scanning, network sniffing, ping floods, packet spoofing, denial of service, social engineering, password cracking and forged routing information.
- For any type of security scanning unless prior authorization is provided by Network Services.
- For executing any form of network monitoring which will intercept data not intended for the user's host, unless this activity is part of the user's normal job duties.
- For circumventing user authentication or security of any host, network or account.
- To alter the College network or system configuration files.
- To copy, alter, or remove College-owned software.
- To copy, alter, or remove files owned by another user.
- To violate the intellectual property rights of others by copying or publishing material in any media. This adherence to copyright laws assumes an informed usage of Fair Use rules. Questions on Fair Use may be referred to the Director of Library Services.
- To interfere with the privacy of others.
- To post or transmit any unlawful or unsolicited message that is threatening, abusive, libelous, obscene, or pornographic, whether in text, audio, or graphic form and regardless of whether or not the message was solicited.
- To obscure or to attempt to hide the identity and location of a remote connection.
- To physically abuse or misuse computing equipment.
- To engage in activities prohibited by local, state, or federal law.

Email Unacceptable Usage Policy:

Examples of unacceptable use of our email system include, but are not limited to, these activities:

- Sending advertising material to individuals who did not specifically request such materials (email spam).
- Any form of harassment via email whether through language, frequency, or size of messages.
- Aside from work-related information or student-based organization information, mass email messages that solicit donations, volunteers or any other type of non-work-related information (i.e., party announcements). Approved campus organizations include FSA, College Foundation and any FSA budgeted student organization.
- Unauthorized use or forging of email header information.
- Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Sending of promotional materials for any non-College related enterprise without permission of the College President.

User Account Creation Procedure:

Student accounts are created when it is determined that a student is registered for a credit-bearing class. User accounts expire after a full calendar year of a student not being registered. Student files will remain available while the account is active. It's the student's responsibility to backup/archive their data before account deactivation.

Faculty and Staff accounts are created when a dean or supervisor submits an Information Technology request form to the Information Technology Department. Banner access is to be authorized by module leaders. The Information Technology request form is available on MyHerkimer.

User Responsibilities:

Along with the privilege of using the College's technology resources come the responsibilities regarding the acquisition and operation of technology resources.

It is the responsibility of each user to ensure that:

- Personal computers or additional computing resources which have been assigned to them (or their office) are controlled and physical security is provided to protect against unauthorized use, damage or loss.

- Rules of any local network administered by Information Technology or wide area network provided such as the internet, or internet service provider to which College resources are used to connect are followed.
- Computer equipment is turned off at the end of the work week, typically Friday.
- Computer equipment is not left unattended or unsecured while in a logged in state.
- Passwords are not revealed to anyone, nor should they allow another person to use their account unless allowed by Information Technology for a specific purpose.
- Passwords should be changed frequently.
- All important files should be saved to your network drive (F or M) before leaving your computer unattended.
- Prior approval is received from Information Technology before any computer equipment assigned to a specific location is installed or relocated.
- Prior approval is received from Information Technology before any maintenance and/or repairs are made to college-owned equipment.
- All requests for computer equipment and/or upgrades for academic or administrative use are submitted in writing during the annual budgeting cycle to the Director of Information Technology.

Roles and Responsibilities of the IT Department pertinent to these Policy & Guidelines:

Information Technology shall be responsible for the following:

- Inform all personnel of our College policies on acceptable use of our information resources and technology.
- Ensure that all personnel under their supervision comply with our policies and procedures.
- Monitor all network/system activities for misuse.
- Promptly report suspicious activities or occurrences of any unauthorized activity.
- Ensure that all policies and procedures are available to all users either in hardcopy or online.

Steps that Information Technology will take to ensure compliance campus-wide:

- Herkimer College owns all the computer facilities and network resources. Use of such resources in any means including non-college devices provides consent for Herkimer College to monitor, inspect, audit and collect any information without permission or further notice. All Herkimer College personnel shall be informed as to what use is acceptable and what is prohibited. Infractions of the Acceptable Use Policy may result in security violations. All Herkimer College users shall be held

personally accountable for such infractions and may be subject to disciplinary action or criminal prosecution.

Herkimer College – Enforcement Policy:

- Violations to this policy will be handled consistently with Herkimer College disciplinary procedures applicable to the relevant persons or departments. Consistent with the Acceptable Use Policy and the Human Resources Department, the College may suspend, block or restrict access to information and network resources when it reasonably appears necessary to do so to protect the integrity, security, and functionality of the College's resources or to protect the College from liability. Herkimer College may routinely monitor network traffic to assure the continued integrity and security of the College resources in accordance with applicable campus policies and laws. The College may also refer suspected violations of applicable law to appropriate law enforcement agencies.

Herkimer College – Abuse Response Policy:

- Incidents of suspected abuse of Herkimer College computing resources should be reported immediately to abuse@herkimer.edu. Information security related questions and issues should be directed to abuse@herkimer.edu.
- Upon receipt of abuse reports, Herkimer College will attempt to verify the abuse, contact the responsible parties, and notify the appropriate authorities.
- Herkimer College may also remove or restrict access for computers, users, or accounts found to be violating the Acceptable Use Policy.

Herkimer College authorities should be notified about violations of computer laws and policies, as well as about potential loopholes in the security of its information systems and networks. When violations are reported, system/network administrators may suspend network privileges pending investigation. Account holders will be notified as soon as reasonably possible. If the violation involves a student, the matter will be referred to the Dean of Students office. If a staff or faculty member commits the alleged violation, the offense will be treated as misconduct under the appropriate section of the Herkimer College Human Resources Policies and Procedures Manual and/or the Faculty/Staff Handbook. Violators of Herkimer College policies or federal, state, or local laws may be denied access to the computer network, in addition to being subject to other applicable disciplinary procedures.