Herkimer County Community College

Department of Information Services

Computer Use Policy and Guidelines

I. General Information:

Computer resources are provided to members of the HCCC community for use in their prescribed tasks as well as for personal and professional development. In order to have access to computer resources, the HCCC Computer Use Policy Acknowledgment/Agreement Form must be signed and returned to the Information Services Department. User accounts are provided on the academic and administrative computing systems (hereinafter called Information Services) as appropriate. Use of these resources is a privilege, not a right, and access is granted with restrictions and responsibilities for their use.

Computer abuse is expensive and can have far-reaching negative consequences from disrupting the educational process to infringing on copyright. Certain misuse of HCCC computer resources can result in revocation of computing privileges, suspension, dismissal and/or criminal prosecution.

It is a mission of the College to promote diversity in values and perspectives, and thus the College is respectful of the freedom of expression. However, the College reserves the right to restrict the use of e-mail in appropriate circumstances in which there may be violations of College policies or 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 the material.

II. Rights and Responsibilities:

Computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege, and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of the systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

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

III. Existing Legal Context:

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

Misuse of computing, networking, or information 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 computing and network 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.

IV. General Access and Use of Computer Labs:

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

- Currently enrolled students of Herkimer County Community College
- Current faculty and staff members of Herkimer County Community 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 HCCC equipment.

Use of computer equipment is subject to the directives given by the person in charge of the lab (faculty or staff member, or technician, or 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 cell phone use is allowed in any computer lab.
• Please respect your peers in regards to the noise level in the lab; others are also trying to study.
• No children are allowed in any computer lab unless part of a formal college activity designed for children.
• At any given time, a lab may be open to individual students or closed to a formal class. Check the window next to the door for the schedule to determine whether a lab is open or closed. No lab should be entered, in which an instructional class is in progress.
• The person on duty may request a valid HCCC ID at any given time while working on a computer in an open lab.
• Students must sign-in and out at the front desk every time they use a lab.
• Students are expected to be polite and courteous to any and all personnel on duty at the time.
• Students’ work should be saved in their personal network account, i.e., the M:\ drive. Save your work frequently; every 15 minutes is recommended. Make sure files are being saved to the My Documents Folder on your personal M:\ drive, not on the C:\ drive.
• Never leave your computer while you are logged into your account. If you must leave even for a short period of time, exit properly from the application (make sure you save your work) and logoff the computer.
• If students are having problems with a computer or printer, they must ask the person on duty for assistance. Students should never attempt to fix the problem.
• If students are having trouble using software, they should ask their Instructor for help. At times a student tutor may be on duty to help. Technicians and work-study staff are not required to help students with assignments and students should not ask them. Technicians are there to ensure that the equipment is operating properly and students are adhering to the rules as defined in this document.

V. Unacceptable and Unauthorized Use:

Unacceptable and unauthorized activities can result in revocation of computing privileges, further disciplinary action, and filing of civil or criminal complaints. HCCC will cooperate with law enforcement authorities in investigations involving criminal activities for which college-owned equipment is employed.

The computing facilities of HCCC and its supporting networks may not be used:

• For access to an account or system you are not authorized to use. This includes obtaining a password for another account without consent of the account owner
  • **For any purpose contrary to the College’s best interests**
• For deliberately wasting computer and network resources
• To interfere with the privacy of others
• 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 computer systems located at HCCC 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 Services or designee

• For the introduction of malicious programs into the network or servers, including but not limited to the following: viruses, worms, Trojan horses, e-mail bombing, e-mail spamming.

• 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 logging into our server or account 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, scanning, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

• For port scanning or security scanning unless prior notification to Herkimer County Community College is made.

• 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 College network 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.

• 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 County Community College.

• 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 interfere with or intercept the electronic communication of another user.

• To obscure or to attempt to obscure the identity and location of a remote connection.

• To physically abuse or misuse HCCC computing equipment.

• To engage in activities prohibited by local, state, or federal law.

VI. Herkimer County Community College – 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, telephone or paging, 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 (ex: party announcements) will be sent to the Webmaster to be posted to the Intranet. Approved campus organizations include FSA, College Foundation and College Alumni Association. Approved student organizations include 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.

VII. User Account Creation Procedure:

Students account creation occurs when it is determined that a student is registered for a credit bearing class. User accounts expire if a student is not registered for a subsequent semester. Student files are normally archived for one month after account termination. It’s the student’s responsibility to backup/archive their data prior to the end of the spring semester

Faculty/Staff Windows account creation occurs when a Dean or Supervisor submits a User Request Authorization Form to the Information Services Department. Forms are available on the College’s Intranet site.

Faculty/Staff Banner account creation occurs when a Dean or Supervisor submits a Computer Account Request form for Banner to the appropriate module leader which is then forwarded to the Information Services Department. Forms are available on the College’s Intranet site.

VIII. User Responsibilities:

Along with the privilege of using the College’s computer resources come the responsibilities regarding the acquisition, operation, and maintenance of computer 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 Services or wide area network provided such as Internet, or Time Warner 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.
• Office phone lines are not used to connect to a PC and modem for accessing any type of remote network such as the Internet.
• Passwords are not revealed to anyone, nor should they allow another person to use their account unless allowed by Information Services for a specific purpose.
• Passwords should be changed frequently.
• Important files that are located on your PC should be backed up frequently.
• Prior approval is received from Information Services before any computer equipment assigned to a specific location is installed or relocated.
• All requests for computer equipment and/or upgrades for academic use are submitted in writing during the annual budgeting cycle to the Academic Computer Committee for review.
• All requests for computer equipment and/or upgrades for administrative use are submitted in writing during the annual budgeting cycle to the Administrative Computer Committee for review.

IX. Roles and Responsibilities of the HCCC Information Services Department pertinent to these Policy & Guidelines:
Information Services shall be responsible for the following:

• Inform all personnel of our campus policies on acceptable use of our information resources
• Ensure that all personnel under their supervision comply with our policies and procedures
• Monitoring all network/system activities for misuse
• Promptly report suspicious activities or occurrences of any unauthorized activity
• Ensure that all our policies and procedures are available to all users either in writing or for online accessibility

X. Steps that Information Services will take to ensure compliance campus wide:

• Herkimer County Community College owns all the computer facilities. Use of such resources provides consent for Herkimer County Community College to monitor, inspect, audit and collect any information without permission or further notice. All Herkimer County Community College personnel shall be informed as to what use is acceptable and what is prohibited. Infractions of corporate acceptable use policies may result in security violations. All Herkimer County Community College users shall be held personally accountable for such infractions and may be subject to disciplinary action or criminal prosecution.
XI. Herkimer County Community College – Enforcement Policy:

- Violations to this policy will be handled consistently with Herkimer County Community College disciplinary procedures applicable to the relevant persons or departments. Consistent with the Computer Use Policy and the Human Resources Department, the College may temporarily suspend, block or restrict access to information and network resources when it reasonably appears necessary to do so in order to protect the integrity, security, or functionality of the college’s resources or to protect the college from liability. Herkimer County Community 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.

XII. Herkimer County Community College – Abuse Response Policy:

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

The Herkimer County Community College authorities should be notified about violations of computer laws and policies, as well as about potential loopholes in the security of its computer 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 Office of Student Affairs. If a staff or faculty member commits the alleged violation, then the offense will be treated as misconduct under the appropriate section of the Herkimer County Community College Human Resources Policies and Procedures Manual or the Faculty/Staff Handbook. Violators of Herkimer County Community 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.

Revised 07/27/09 – Version 3.11