



## **Acceptable Use Policy**

Last Revision: July 31, 2007

**College Information Technology Services**



## **I. Introduction**

In keeping with Erie Community College (ECC) mission and goals, a variety of information technology resources are offered to provide accessible, affordable, quality education and services to a diverse community that includes students, faculty and staff. The capabilities these resources offer include, but are not limited to, network and local computing, telephony and video conferencing. They are supported through workstations, servers, networks, phones, video conference units and other information technology devices and peripherals. Information technology resources are intended for college-related purposes, including direct and indirect support of academics, research and service missions, college administrative functions, student and campus activities and the free exchange of ideas within the college community and the wider local, national and world communities.

The policy contained herein applies to all faculty, staff, students and other authorized users of ECC's information technology resources. Additional policies may govern certain computing resources, such as workstations, network devices, servers or computer labs. Users are encouraged to consult the manager or administrator responsible for those services to obtain further information. This policy supplements all applicable State University of New York (SUNY) policies, existing college policies and federal, state and local laws. Please note that the policy may be modified as deemed appropriate by Erie Community College. Users are encouraged to periodically review this policy posted on the college website at <http://www.ecc.edu>.

## **II. Authorized Use**

ECC's computer facilities are a resource for members of the campus community, to be utilized for activities consistent with the instructional, research, and administrative goals of the College.

As a condition for use of the computing facilities, all users must adhere to the regulations below.

- **Authorized Activities**

ECC computer facilities shall be utilized solely for work consistent with the instructional, research, and administrative goals of the College, as defined in the ECC "Missions and Goals" statement.

- **User Privacy**

Users shall respect the privacy of others. Users should not intentionally view information of other users, modify or obtain copies of other users' files, or modify other users' passwords without their permission. ECC computers and networks are designed to protect user privacy; users shall not attempt to circumvent these protections.

- **Resource Accounting**

Users will not develop or use procedures to alter or avoid the accounting and monitoring of the use of computing facilities. For example, users may not utilize facilities anonymously or by means of an alias, and may not send messages, mail, or print files that do not show the correct username of the user performing the operation.

- **Resource Usage**

Users must use the computing facilities in a responsible and efficient manner. Users are not permitted to alter the lab microcomputers in any way. They are expected to refrain from deliberately wasteful practices such as printing unnecessary listings, performing endless unnecessary computations, or unnecessarily holding public terminals for long periods of time when others are waiting for the same resources. Users are not allowed to develop or use procedures that obstruct authorized use by others. Users shall not interfere with microcomputer setups which are intended to keep microcomputer software current and legal.

- **Copyrights and Licenses**

Users may not violate the legal protection provided by copyrights and licenses held by ECC. Users should not make copies of any licensed or copyrighted computer program found on any ECC computer or storage device without the written authorization from the College Information Technology Services (CITS) department. US Federal copyright law grants authors certain exclusive rights of reproduction, adaptation, distribution, performance, display, attribution, and integrity to their creations. Works of literature, photographs, music, software, film, and video works can all be copyrighted. Examples of probable violations of copyright laws include, but are not limited to: making unauthorized copies of any copyrighted material (such as commercial

software, text, graphic images, audio, and video recordings); distributing copyrighted materials over computer networks or through other means; resale of data or programs, or the use of them for non-educational purposes or for financial gain; public disclosure of information about programs (e.g. source code) without the owner's authorization.

- **Anti-Virus Protection**

Every computer connected to the campus network will be required to run current anti-virus protection software. Campus-provided "managed" anti-virus protection is placed on all campus-owned computers.

### III. Unauthorized Use

- **Unauthorized Activities**

Users may not engage in wasteful and/or illegal practices which abuse the computers or networks. These practices include, but are not limited to, the following:

- Game Playing - While limited game playing is permitted, users are not allowed to engage in recreational or competitive game playing which utilize computing and network resources.
- Viruses – Users are not allowed to create or knowingly distribute viruses to other users, or propagate viruses through the ECC network or Internet.
- Chain and Hoax Letters – Under no circumstances will users distribute chain or hoax e-mails.
- Unauthorized Servers – The establishment of a background application which services incoming requests from other users for the purpose of gaming, chatting, browsing the web or transferring files is prohibited.
- Unauthorized Monitoring – A user may not use computing resource to monitor or capture any electronic communication.
- Spamming or Flooding – The use of ECC's e-mail system to send out unsolicited mail, or multiple mail messages to list servers or newsgroups with the intent of reaching as many people as possible is strictly prohibited.
- Private Commercial Business – Computing resources will not be used for personal or private commercial business or for financial gain.
- Political Advertising or Campaigning – ECC's computer resources cannot be used for any type of political advertising or campaigning.
- Repair or Move Computers – Users may not attempt to repair or move any computer, network device or peripheral without proper authorization.
- Circumventing Security Measures – Users are prohibited from circumventing or attempting to circumvent any system or computing security measures. This includes any software or hardware device which intercepts or decodes passwords or similar access control information.
- Unauthorized Access – Users are not permitted to use computing resources to gain unauthorized access to remote computers or to impair or damage the operation of ECC's computers, network or peripherals. This includes blocking communication lines, intercepting communications, and running, installing or sharing virus programs. Users must not offer alternative methods of accessing ECC network resources, such as through dial-up or VPN.
- Network Device Installation – Users must not implement any device or computer on the network without proper authorization. This includes, but is not limited to, laptops, hubs, switches, routers, firewalls and wireless access points.
- Terrorism – Users are not allowed to use ECC's computing resources to participate in any terrorist discussions, actions and/or activities connected with overthrowing the government of the United States.

- **Academic Dishonesty**

Practicing any form of dishonesty through use of computing facilities (for example cheating, plagiarism, or fraud) is prohibited.

- **Harassment**

Using computers or networks to harass, abuse or intimidate another person is prohibited. Users shall not develop or employ programs that harass other users. Users shall be sensitive to the public nature of shared facilities, and take care not to display on screens in such locations images, sounds or messages that could create an atmosphere of discomfort or harassment for others.

- **Obscenity**

Obscene language in electronic mail, messages, process names, file names, file data, and other publicly visible forms is prohibited.

- **Pornography**

Pornography in electronic mail, file data, web sites, and other publicly visible forms, is prohibited. Federal Child Pornography Law makes it illegal to create, possess, or distribute graphic depiction of minors engaged in sexual activity, including computer graphics. Computers storing such information can be seized as evidence.

#### **IV. Electronic Mail**

The purpose of this policy is to ensure the proper use of ECC's e-mail system by its students, faculty, and staff. Electronic Mail is a tool provided by the college to complement traditional methods of communications and to improve education and administrative efficiency. Users have the responsibility to use this resource in an efficient, effective, ethical and lawful manner. Use of the college's e-mail system evidences the user's agreement to be bound by this policy. Violations of the policy may result in restriction of access to ECC's e-mail system and/or other appropriate disciplinary action.

- Erie Community College owns all e-mail accounts run on its system. The College Information Technology Services department is responsible for maintaining the system.
- While incidental non-business personal use of e-mail is acceptable; conducting business for profit using College resources is forbidden.
- While the College will make every attempt to keep e-mail messages secure, privacy is not guaranteed and users should have no general expectation of privacy in e-mail messages sent through the Institutional system. Under certain circumstances, it may be necessary for the CITS staff or other appropriate campus officials to access email files to maintain the system, to investigate security or abuse incidents or violations of this or other college policies. Such access will be on an as needed basis and any e-mail accessed will only be disclosed to those individuals with a need to know or as required by law.
- Individuals are responsible for saving e-mail messages as they deem appropriate. Due to limited resources, the ECC CITS department has the right to restrict the amount of user space on the e-mail server as necessary and to purge and remove e-mail accounts of students who have not registered for a semester, as well as for other individuals no longer affiliated with the college.
- When using e-mail as an official means of communication, students, faculty, and staff should apply the same professionalism, discretion, and standards that they would use in written business communication. Furthermore, students, faculty, and staff should not communicate anything via e-mail that they would not be prepared to say publicly.
- Approval and transmission of e-mail containing essential college announcements to students, faculty, and/or staff must be obtained from the appropriate authority. Only the Offices of Vice President or President can authorize the sending of broadcast messages to a wide audience of students, faculty, and staff within the scope of their authority.
- Any inappropriate e-mail, examples of which are described below and elsewhere in this policy, is prohibited.
  - The creation and exchange of messages that contain harassing, obscene or threatening material.
  - The unauthorized exchange of proprietary information or any other privileged, confidential or sensitive information.

- The creation and exchange of advertisements, solicitations, chain letters and other unofficial, unsolicited e-mail.
- The creation and exchange of information in violation of any laws, including copyright laws, or Institutional policies.
- The knowing transmission of a message containing a computer virus.
- The misrepresentation of the identity of the sender of an e-mail.
- The use or attempt to use the accounts of others without their permission.

## **V. Password Use**

- Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of Erie Community College's entire network.
- This policy is intended for every employee and student who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any Erie Community College facility, has access to the college's network, or stores any non-public ECC information.
- Passwords must not be inserted into email messages or other forms of electronic communication, nor are they allowed to be written down and kept in an unsecured location (e.g., such as on a post it note on your desk).
- All user-level and system-level passwords should conform to the guidelines described below.

*Strong passwords have the following characteristics:*

- Contain both upper and lower case characters (e.g., a-z, A-Z)
- Have digits and punctuation characters as well as letters e.g., 0-9, !@#%&\*()\_+|--=\`{}[]:~';<>?,./)
- Are at least eight alphanumeric characters in length.
- Is not a word in any language, or found in the dictionary.
- Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

*Poor, weak passwords have the following characteristics:*

- The password contains less than eight characters
- The password is a word found in a dictionary (English or foreign)
- The password is a common usage word such as:
  - Names of family, pets, friends, co-workers, sport teams, etc.
  - Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
- If an account or password is suspected to have been compromised, report the incident to the CITS Helpdesk and change all passwords ASAP.

## **VI. Violations**

Users should notify the Vice President of Information Technology's office, Network Administration Office, a classroom instructor, lab monitor or supervisor of any intentional or unintentional breaches in security. In addition, users may E-mail [abuse@ecc.edu](mailto:abuse@ecc.edu) regarding any violations of this policy.

All suspected violations will be presented to the appropriate College official to determine whether a violation of this policy occurred. If the College official determines a violation occurred, the users account may be immediately suspended, or their privileges may be revoked in addition to other remedial actions. If warranted, other sanctions may be imposed including suspension or expulsion from Erie Community College. Any violations of local, state or federal law will be dealt with by the proper authorities



