Committee Meeting: Policy Committee	Date: March 3, 2017
Committee Chair: Kathleen Masiello-members present listed on page 8	
New or Edited: Edited CITS Acceptable Use Policy	

POLICY NAME: Information Technology Services Acceptable Use Policy

POLICY TYPE: Managerial

SUBMITTED BY: Maria Carroll (Human Resources) & Joseph Lundin (Information Technology Services)

ISSUE OR STATEMENT OF PURPOSE:

The existing Information Technology Services (hereinafter "ITS") Acceptable Use Policy is outdated and needed to be expanded/updated to appropriately address issues surrounding use of College technology resources. All employees acknowledge this policy when logging into the network etc. This policy governs use of campus technology and resources and is for all users.

CORRECTIVE ACTION PLAN RECOMMENDATION (if any):

NEW OR EDITED POLICY: Edited

INTRODUCTION:

SUNY Erie Community College (hereinafter "SUNY Erie") provides its students and employees wide access to information and technology resources. With the advent of new forms of technology, SUNY Erie has recognized that making technology resources more accessible furthers the free exchange of opinions and ideas essential to academic freedom and the mission of the College.

Technological resources are shared by all users; misuse of these resources even by a single user infringes upon the opportunities for the entire college community. SUNY Erie is a public institution of higher education, and as such, it is incumbent on all users to employ the college's resources properly. The College makes its technology available for educational purposes, requires users to observe state, federal, and other legal regulations to safeguard privacy (i.e. HIPAA, FERPA, etc.), maintain equipment, protect networks, data and software acquired and to maximize its spending of public funds. Proper and fair use is essential if all are to benefit from these resources.

Information Technology Services (hereinafter "ITS") provides and maintains the campus network, servers, computer labs and facilities, and College-owned equipment such as telephones, desktop and laptop computers. ITS provides additional services, including the operation of a Help Desk, tutorial assistance, audiovisual services and educational technology resources and support. These facilities and technological resources and services provided through ITS are a crucial resource for academic and administrative members of the college community.

POLICY NAME: Information Technology Services Acceptable Use **- Continued**

Use of College ITS resources is considered an agreement to abide by this policy. Users found in violation may be subject to penalties of varying degree, and violators may also be subject to action by college, civil, or criminal judicial systems.

This document establishes rules and prohibitions that define acceptable use of all CITS resources.

The College reserves the right to amend this policy at any time. Users should routinely review this policy throughout the year to ensure they are up to date on its requirements.

PRINCIPLES:

The college respects individual privacy, civility, and intellectual property rights.

Since no list can cover all possible circumstances, the spirit of this policy must be respected, namely; any action that hinders legitimate equipment usage, hinders one's work performance unnecessarily, circumvents security measures or invades the privacy of another person or institution is unacceptable.

User Responsibilities & Privacy Considerations:

All college faculty, staff, and students are afforded the privilege of access to the computing and network resources/equipment of the College. Such access may be granted to other individuals with approval from ITS or library personnel. All parties are responsible for preserving the integrity of the College's IT resources and using them in a manner consistent with this policy, any other applicable ECC policies and relevant federal, state and local laws and regulations.

a. Users accept responsibility for learning how to use information technology effectively and responsibly. The College provides training on the use of information technology. All users are encouraged to learn the proper use of information technology through individual learning or by attending training sessions or classes.

b. Users accept responsibility for backup and security of their own work. Each user should learn how to make backup copies of important work and to properly use software features for securing or sharing access to their information.

c. Users acknowledge that SUNY Erie does not routinely monitor, inspect or disclose the content of individual usage of College IT resources except under limited circumstances. As such, absent permission by a user, the College reserves the right to monitor or inspect system resources, including equipment, activity and accounts, with or without notice, when:

> 1. It appears reasonably necessary to protect the integrity, security, or functionality of College resources or to protect SUNY Erie from liability.

2. An account or system is engaged in unusual or excessive activity.

3. There is reasonable cause to believe that regulations, policies, contracts, or laws are being violated.

4. In the event of health, safety, or security emergencies, as determined by authorized College officials.

5. When it is necessary to retrieve vital college-related material following verification by the appropriate member of Human Resources or other authorized College official of: 1)the extended absence of an employee, 2) the demise of an employee, 3) investigation into misconduct, or 4) the termination of an employee for cause.

6. It is otherwise required or permitted by law.

Any access as outlined in the preceding will be done in consultation with the Erie County Attorney, SUNY Erie's Chief Information Officer/Vice Provost, the AVP of Human Resources (for employees), and/or Vice Provost or authorized Dean(s) of Students (for students).

Any access made to an individual's account or data will be no more extensive than necessary.

The normal operation and maintenance of the College's computing resources requires the backup of data, the logging of activity, the monitoring of general usage patterns, and other such activities as may be necessary in order to provide desired services.

d. Equipment (e.g. laptops, desktop computers, tablets, cell phones, etc.) assigned to faculty and staff for the duration of their employment at SUNY Erie remain the property of SUNY Erie and should be treated as such. These devices may be upgraded, as warranted, and must be relinquished in order for any required repairs or updates to be performed.

All SUNY Erie personnel are strongly encouraged to use College-provided resources only for SUNY Erie business- related material and to acquire and use personal email accounts and electronic devices for any non-work related material.

Note that equipment failure or circumstances such as suspension or termination of employment could result in the immediate inability to access one's assigned computer or equipment. Accordingly, users are encouraged to use personally-owned equipment, rather than College equipment, to store or process personal materials.

Voluntarily separating employees should review the "SUNY Erie Off boarding Policy" to review the process for the return of technological equipment, which is required before one's last day of work.

Use of College Technology Facilities

a. All technology facilities of the College, including those located in remote sites, are for the use of SUNY Erie students, employees, Trustees and other authorized users from the community.

b. Users must not abuse equipment and are asked to report any mistreatment or vandalism of computing or network facilities to ITS staff or to Security.

c. Food is discouraged in all computing facilities because of potential harm to equipment. Beverages in approved containers (sturdy, covered, reusable containers) are allowed.

d. Users should relinquish the computer they are using if they are doing nonessential work when others are waiting for a computer to perform course or work-related activities. Equipment should not be monopolized. Users should not use more than one computer at a time and should plan work so that the computer session is no longer than absolutely necessary.

e. Game playing in ITS-maintained computer facilities/labs is prohibited at all times.

f. Users should not install software, alter system files, move, or disconnect any cables on computers or other equipment.

g. Users are expected to respect other users and the staff of the computer labs. Harassment or verbal or physical abuse of others, student or staff, will not be tolerated.

h. A user must show a SUNY Erie ID card to any SUNY Erie staff member or student employee upon request.

i. Users must respect all notices (such as those concerning hours of operation, printing, etc.) posted in technology facilities.

Legal Usage

a. Information technology resources may not be used for illegal or harmful purposes, including, but not limited to:

   i. Intentional harassment of others. 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.

   ii. Intentional destruction or damage to equipment, software, or data;

iii. Intentional disruption or unauthorized monitoring of electronic communications;

iv. Other illegal acts, including 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.

b. Software licensed by the College must only be used in accordance with the applicable license agreements. Software is normally distributed under three kinds of licenses: proprietary, public distribution, and shareware. Unless otherwise indicated, users should assume all software made available by ITS is proprietary and may not be legally copied.

c. ITS will not knowingly provide support for software that a user possesses in violation of its license agreement. Consultants and staff may ask for proof of ownership before helping users with their software.

d. ITS will not knowingly allow illegally acquired software to be used on ECC-owned computers. ITS will remove any suspect software loaded onto SUNY Erie-owned computers or servers.

e. ITS will not knowingly allow use of its resources (computers, equipment, network, etc.) for the illegal copying of digital media or files. Note: U.S. Copyright Law protects copyright owners from the unauthorized reproduction, adaptation, or distribution of digital material, including the unauthorized use of copyrighted sound recordings (e.g., music files), video files, and interactive digital software (i.e., video games).

Ethical Usage

a. Users should not use information technology resources, including personally-owned computers connected to the college network, for non-college, unsanctioned, commercial activity, political advertising or campaigning.

b. Users should make no attempt to alter the condition or status of any computing network component in any manner.

c. Users should make no attempt to alter software other than their own, or to copy software intended only for execution.

d. Users should not interfere with, interrupt, or obstruct the ability of others to use the network or other ITS resources.

e. Users should not attempt to connect to a host via the network without explicit permission of the owner.

f. Users should not provide, assist in, or gain unauthorized access to SUNY Erie computing or network resources.

g. Users should not attempt to circumvent or defeat computer or network security measures.

h. Users should not systematically collect and use any privately or publicly available college data or content, including users' personal directory and account information, through the use of data mining, robots, or similar gathering and extraction methods.

Security

The college uses various measures to ensure the security of its computing resources. Users should be aware that the college cannot guarantee such security and should apply appropriate safeguards for their accounts, such as guarding their passwords and changing passwords regularly (required for network and ERP system accounts), and logging out of computers when done.

All user and system passwords should conform to the guidelines described below:

- The password should contain both upper and lower case characters (i.e.: a-z, A-Z)
- Numbers and special characters should be used in combination with letters (i.e.: 0-9, !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)
- At a minimum, passwords should be at least eight alphanumeric characters in length.
- The password should not contain a word in any language, or be found in the dictionary.

Any user who believes their SUNY Erie account or equipment has been compromised should immediately contact the ITS Helpdesk.

Account Usage

a. Account holders should use only their own personal SUNY Erie accounts, unless given express permission by an authorized member of the faculty, administration, or professional staff to use a general account that is designated for a specific purpose or job.

b. Account holders may not allow others to use their personal SUNY Erie accounts. The person holding an account is responsible for its use, and all activity originating from that account, at all times.

c. Account holders should protect their passwords and keep them confidential. Passwords should be changed frequently and never written down. Any security breaches, such as theft of data or a system compromise, resulting from irresponsible use of a password (e.g., a password that can be easily guessed or oral or written dissemination of a password) may be treated as grounds for action against the account holder, which may include discipline and/or suspension of account privileges. Any attempt to determine the passwords of other users is strictly prohibited.

d. Account holders should not abuse any email, forums, or communications system, either local or remote,

by sending rude, obscene, or harassing messages (including chain letters and hoax messages) or by using these systems for non-essential purposes during the times when the computers are in heavy demand. Account holders should identify themselves clearly and accurately in all electronic communications, e.g., no anonymous postings and no spoofing of addresses. Unofficial mass e-mailings (i.e., spam) are prohibited.

e. Individual SUNY Erie accounts (@ecc.edu mail accounts, web accounts, applicant system accounts, etc.) are created for the express use of the individual for whom the accounts are created, but remain the property of SUNY Erie. Accounts may be viewed in circumstances such as those enumerated in prior sections of this policy. All business-related correspondence should take place using one's SUNY Erie email address, because as a public employer, we are subject to laws regarding public record.

Network Usage

The following are responsibilities that are particularly applicable to users of SUNY Erie's campus-wide network.

a. Only computers that have been properly virus checked, updated, and authenticated through established procedures may be connected to the campus network, unless otherwise authorized and established by ITS. Users must not attempt to circumvent this process.

b. The person recognized as the owner of that authenticated computer system is responsible for that computer's use, and all activity originating from that computer, at all times.

c. Excessive or improper use of network resources that inhibits or interferes with use by others is prohibited and will be cause for action by ITS, which may include restricting, limiting, or disabling network access.

d. Users who connect computers to the network that act as servers have the additional responsibility to respond to any use of their server that is found to be in violation of this Policy.

e. In no case shall the following types of servers be connected to the network: DNS, DHCP, BOOTP, or any other server that manages network addresses.

f. Due to the serious negative impact on network availability created by misconfigured routers and Wireless Access Points (WAPs), all routers and WAPS, except those configured and used by CITS, or devices which function as routers or WAPs, are disallowed.

Enforcement

The College in its discretion is the sole arbiter of what may constitute a violation of this policy.

Violations of this Policy will be adjudicated, as deemed appropriate, and may include the following:

a. Loss of computing privileges

b. Disconnection from the network

c. Disciplinary action

d. Prosecution under applicable civil or criminal laws

RELATED DOCUMENTS

1. SUNY Erie Employee Off boarding Procedures
2. Erie County Employee Handbook – Removal and Disciplinary Action

CONTACTS

Questions regarding the terms of this policy should be directed to:

ITS   716-851-1977
Human Resources   716-851-1840

DOES IT SUPERCEDE A POLICY/WHICH ONE: Existing SUNY Erie CITS Acceptable Use Policy.

POLICY COMMITTEE RECOMMENDED ACTION: Approved as amended above. Policy Committee recommends the Board of Trustees accepts the Managerial policy under the Report of the Chair, Ad Hoc Committee Reports, and Policy Committee. This Policy supersedes all prior policies/procedures and practices related to ITS Acceptable Use Policy.

POLICY COMMITTEE MEMBERS PRESENT: Trustees Kathleen Masiello, Executive Vice President of Operations Michael Pietkiewicz, Chief Financial Officer and Senior VP of Administration and Finance William Reuter, Director of Human Resources Tracey Cleveland, Vice President of Enrollment Management Erik D'Aquino

DATE OF BOARD ACCEPTANCE: March 30, 2017

POLICY COMMITTEE TEAM FOLLOW-UP: Distribution of new policy to employees and to new hires at orientation.

INFORMATION/INPUT CONSIDERED DURING POLICY COMMITTEE DELIBERATIONS:
Policies from Oberlin College and Clinton Community College were used to create this revised policy.

This Policy has been previously reviewed and discussed at the Policy Committee meetings of October 25, 2016 and November 01, 2016. At the meeting of March 3, 2017 the Policy committee unanimously approved this Policy with edits that have been made to the above.