EASTERN GATEWAY
COMMUNITY COLLEGE

Network, Computer Resources and the Internet Acceptable Use Policy for Students and College Guests

1.0 POLICY OVERVIEW

1.1. Access to Eastern Gateway Community College's (the college) networking facilities, computer resources and the internet is a privilege. The college's network, computer resources and the internet are provided solely to support its educational mission.

1.2. This policy is to be read, understood and adhered to at all time. Local, state and federal laws regarding the use of internet, e-mail and any other networking or computer resources made available by the college are also applicable.

1.3. The college insists that you conduct yourself honestly and appropriately when using the college's network, computer resources and the internet. You are to comply with software licensing rules, property rights, copyrights and the privacy and prerogatives of others.

1.4. All existing college policies related to plagiarism, sexual harassment, privacy and confidentiality also apply to your use of the college's network, computer resources, and the internet.

1.5. The college reserves the right to revoke all network privileges for any user at any time for violation of this policy.

2.0 VIOLATIONS

2.1 The following is a summary of violations of the acceptable use policy. The examples are not all inclusive.

2.1.1. Lending your account and/or accessing another person's account without permission.

2.1.2. Using illicit means to determine account passwords.

2.1.3. Attempting to gain access to the network or computer resources with nonstandard or non-approved procedures.

2.1.4. Using the college's network, computer resources or the internet for commercial purposes.

2.1.5. Using the college's network, computer resources, or the internet to threaten, intimidate, or harass others.

2.1.6. Attempting to thwart computer system security in order to gain unauthorized access to the network or computer resources.

2.1.7. Unauthorized copying of commercial software when specific licensure prohibits such copying.

2.1.8. Sending chain letters or unauthorized mail list generation.

2.1.9. Placing obscene or harassing material so that it is accessible in public areas of the network.

2.2.0. Inspecting, modifying, or copying programs and/or data without proper consent and respect for copyright laws.

2.2.1. Tampering with the college's hardware, software, or other computer components.

2.2.2. Accessing or reading information of others without direct consent (this includes packet sniffing).

2.2.3. Providing other individuals with access to Eastern Gateway Community College network resources without direct consent from the Technology Services Department.

2.2.4. Authenticating as or impersonating another individual via e-mail or other methods.

2.2.5. Attempting to degrade or disrupt network and/or system performance.

3.0 SECURITY, PRIVACY AND COPYRIGHTS

3.1. The college will provide as secure of an environment on its networks as is possible. Security will be provided using widely accepted, cost effective methods for all network users. Network users must recognize that as a participant in a community data facility, they also must be partially responsible for maintaining the security of information stored or retrieved via the college network. Information is a valuable resource and should be considered an entity worth protecting by using good judgment and respecting the policies and procedures in place at the college.

3.2. Data owned by others should be considered private and no attempt should be made to gain access to another's information. Care should be taken when reading, forwarding and printing electronic messages. Interfering with e-mail in any manner is a serious offense. Sharing of your network account places your data at risk. Always keep your password secure and select a unique password that cannot be easily discovered by others. Extreme care and responsible use of computer resources is required of all users. Each network user must be aware of the existence of copyright laws, licenses, trade secret agreements and other confidentiality agreements as they pertain to the resources they may access using the college network.

3.3. The college has made network resources available to the college community members with specific attention to ensure that the rights of all users are protected. Users who are granted access to the college network, including the hardware and software made available for network connectivity, agree to abide by the college's acceptable use policy.

3.4. The Technology Services department will establish and publicize the acceptable use policies and procedures. Secure access to the network will be provided using a network login and a user maintained password. The college will provide anti-virus software for each college-owned computer attached to the network.

4.0 SECURITY, NETWORK AND INTERNET MONITORING

4.1. The college has security software and systems in place that can monitor and record network and internet usage. These systems are used to protect the college's network systems from security risks

and software viruses. Our firewall and other systems record all internet traffic in and out of the college. This information can be used to monitor security violations and network bandwidth utilization. This information is also used to configure our networks and internet connection for optimum operation. Network usage information may also be used to insure compliance with college policies and procedures.

4.2. The college's network facilities are for the use of authorized users only. Individuals using the college's network facilities without authority, or in violation of stated policies, are subject to having all of their activities on the network monitored and recorded by system personnel. In the course of monitoring individuals improperly using network facilities, or in the course of system maintenance, the activities of other users may also be monitored. Users accessing the college's network consent to monitoring as stated in the Electronic Communications Privacy Act, 18 USC 2701-2711. Anyone using the college's network facilities expressly consents to such monitoring and understands that if such monitoring reveals violations of college policies and/or local, state and federal laws, such information may be provided to appropriate college and/or law enforcement officials.

4.3. The college reserves the right to limit (or block) access to certain internet sites and applications if it is determined that such access does not support its educational mission or is detrimental to the operation of the college's network systems. The college reserves the right to make all decisions regarding the necessity and appropriateness of access to specific internet sites and applications.

5.0 ILLEGAL ACTIVITIES

5.1. The college's network, computer resources and internet access must not be used to knowingly violate the laws and regulations of the United States or any other nation, or the laws and regulations of any state, city, province or other local jurisdiction in any material way. Use of any college resources for illegal activity is grounds for immediate expulsion or dismissal, and we will cooperate with any legitimate law enforcement activity.

6.0 PASSWORD PROTECTION

6.1. Each user is required to password protect his/her network account. It is advisable to protect your network account with a password and maintain the confidentiality of all passwords associated with your computing resources. It is strongly recommended that you use passwords that would be difficult to guess (e.g. not the names of family members, pets, etc.) It is also recommended that your password contain both numbers and alphabetic characters.

7.0 SEXUAL HARASSMENT

7.1. The display of any kind of sexually explicit image or document that can be seen by others (either intentionally or accidentally) on any college computer system is a violation of our policy on sexual harassment. In addition, sexually explicit material may not be archived, distributed, edited, or recorded using the college's network, computing resources or the internet.

8.0 GAME PLAYING

8.1. The college's networking facilities exist to support the educational mission of the college. Therefore,

game playing and recreational chatting are discouraged. Users must relinquish their computer to other users needing network access for educational pursuits. Users of college computers must also cease from such activities if requested to do so by an official of the college or employee thereof (this includes requests from student lab assistants). Failure to abide by these regulations shall be considered a violation of the college's acceptable use policy.

9.0 ILLEGAL SOFTWARE

9.1. No person may use the college's network, computer resources or internet facilities to download or distribute pirated software or data. In addition, all users of the college's network facilities are expected to abide by software licensing rules and regulations. All software on college computers must be legally licensed.

10.0 HOSTING OF WEB SERVICES, FTP, ETC.

10.1. No person may set up or provide the hosting of internet Web, FTP or related services on the college's network without prior consent from the Technology Services department.

11.0 LOGGING OFF OF NETWORKS

11.1. All users must LOG OFF the college's networks when they are not actively using the services of such networks. User logins that span extended periods of time with no activity will not be allowed and will be considered violations of network policy and procedure.

12.0 USE OF COLLEGE PRINTING EQUIPMENT

12.1. The college's network printers are provided in support of the college's educational mission. College printers shall not be used for commercial purposes. Users may print personal e-mail messages, internet documents, etc., as long as they are not unreasonable in size or quantity. *College printers shall not be used to produce more than three (3) copies of any single document* (this does not include rough drafts, etc.) *unless prior permission has been received from the Technology Services Department.* Photocopy machines should be used for producing multiple copies of the same document.

12.2. If you question whether the printing of a particular document is in violation of this policy, please contact the Technology Services department.

13.0 REMOTE ACCESS RESTRICTIONS

13.1. No person shall provide remote access to the college's networking facilities without direct permission from the Technology Services department. This would include the use of modems for dialing in to computers connected to the college's networks. Unauthorized remote access presents a serious security threat and will be considered a serious violation of the acceptable use policy. Any computer that is configured to provide dial-in access via a modem must be physically removed from the college's network unless permission has been granted from the Technology Services Department.

14.0 INSTALLATION OF SOFTWARE ON COLLEGE COMPUTERS

14.1. It is a violation of college policy to install or attempt to install any software on college-owned computers without direct permission from the Technology Services department.

15.0 E-MAIL, USAGE, PRIVACY AND STORAGE

15.1. Electronic mail messages are considered by the college to have the same privacy protection as corresponding paper documents. Violation of the privacy of a user's e-mail documents will be considered a serious offense of the college's acceptable use policy. Users should act to protect their privacy by maintaining passwords and logging off the network immediately after each use. The privacy of e-mail for college constituents will be upheld in accordance with federal, state and local laws.

15.2. Tampering with the college's e-mail system or the e-mail of other users will be considered a serious offense. This includes imitating or 'spoofing' someone else when sending e-mail. The college's e-mail system shall not be used for unsolicited mail (i.e. 'spamming'). Please be advised that many mail systems will return undeliverable mail to the 'postmaster' at its intended destination. This mail message may include all or a portion of the original message.

15.3. Users should act responsibly by purging read and unwanted e-mail from the system. Users should also actively manage and maintain e-mail that is coming in from automated mailing lists, etc. Users should unsubscribe from mailing lists and other automated resources when they will be unable to check their mail for extended periods of time.

15.4. The forwarding and distribution of chain letters and pyramid schemes via email is prohibited at the college.

16.0 ACTIVITIES DETRIMENTAL TO NETWORK PERFORMANCE

16.1. The college reserves the right to prohibit any use of the college's network facilities that it deems detrimental to the performance and operation of the college's networks. Examples might include recreational uses of the network which consume an excessive amount of network bandwidth, etc.

17.0 WiFi CONNECTIONS

17.1. Students and guests of the college may utilize the WiFi technology that is available on campus and will receive troubleshooting and technical support from the college's Technology Services department.

17.2. Students and guests are responsible for obtaining their own network adapter for use during their enrollment.

17.3. Students and guests are required to have updated anti-virus software installed and active at all times they are connected to the college network. Not utilizing the proper anti-virus software may result in revocation of networking privileges.

17.4. Students and guests are ultimately responsible for the repair and maintenance of their own WiFi

enabled device.

17.5. By connecting to the college's WiFi network, students and guests agree to the terms of this policy and that they are using the network at their own risk.

17.6. Protection of college computing resources from computer viruses and other malicious software is a high priority. Each user accessing the network is required to have anti-virus protection installed and operating on the WiFi enabled device they are using. All file input and output activity must be scanned for viruses to prevent network infection.

18.0 COMPUTER LABS AND CLASSROOMS

18.1. In addition to the policies and procedures listed previously, the following apply to the college's computer labs and classrooms:

18.1.1. No eating, drinking, or smoking is permitted within college computer labs or computer classrooms.

18.1.2. No activities which disrupt the activities of others are allowed. (This includes the playing of music, applications which make noise, etc.). Portable devices with earphones are allowed if they do not interfere with others. Respect your neighbor.

18.1.3. All trash, paper scraps, etc. should be deposited in the appropriate trash and recycling receptacles. Please help keep these areas clean.

18.1.4. Lab and classroom users should close all programs and log off the computer when their work is completed.

18.1.5. Report all problems, etc. to Technology Services. If this is not possible, contact a college official. You may also e-mail to tshelp@egcc.edu.

18.1.6. Do not take unused paper from the lab (other than scrap from the recycling receptacles). Unauthorized removal of paper will be considered theft and dealt with accordingly.

18.1.7. Do not tamper with, alter or destroy any hardware and/or software in the college's computer labs, computer classrooms.

19.0 NOTIFICATION OF VIOLATION OF POLICIES AND PROCEDURES

19.1. The college reserves the right to revoke network privileges for any user at any time. If the violation is of a non-critical nature, the Technology Services department or another appropriate official of the college will notify you at least once. Repeat violations will result in suspension or revocation of network privileges.

20.0 UPDATES TO POLICIES AND PROCEDURES

20.1. As a college network user, it is your responsibility to remain fully aware of changes to the college's acceptable use policy. A complete and up-to-date version of all the college's acceptable use policy will be available on Eastern Gateway Community College's web site at www.egcc.edu.

21.0 QUESTIONS REGARDING ACCEPTABLE USES

21.1. If you do not fully understand any policy or procedure listed as part of the college's acceptable use policy, you are responsible for seeking clarification from the Technology Services department. In addition, you are responsible for contacting the Technology Services department if you have questions regarding any use of the network, computer resources and the internet that are not explicitly described in the policies and procedures document. The Technology Services department may be contacted as follows:

E-mail:

tshelp@egcc.edu

Mail:

Eastern Gateway Community College
Technology Services Dept.
4000 Sunset Blvd.
Steubenville, Ohio 43952