ACCEPTABLE USE OF INFORMATION SYSTEMS

General Principles

Having access to computer systems and networks owned or operated by Holyoke Community College imposes certain responsibilities and obligations and is granted subject to College policies, local, state and federal laws. Acceptable use always is ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy. Additionally, the privilege of accessing the college's computer networks carries certain responsibilities for all users of desktop and laptop computing systems. These include, but are not limited to, performing required operating system updates, ensuring proper anti-virus software is installed and periodically run, maintaining adequate data backups and protecting the systems integrity.

1. Guidelines

In making acceptable use of resources you must:

- never place hardware or software, from an outside vendor or private party on the network. All computers accessing the campus network from on campus must be purchased, maintained, screened, secured and set up for operation by ITD.
- individual end users are personally responsible for their data backups and storage. ITD plays no role in the management of end user data, but will provide training during orientation and other course offerings.
- use resources only for College business and for purposes authorized by the College.
- end users are responsible for all activities on your user account or that originate from your system that result from your negligent failure to protect your user account or to protect against such unauthorized use.
- access only files and data that are your own, that are publicly available, or to which you have been given authorized access.
- be familiar with social engineering techniques, such as those used in phishing, spear phishing and spoofing.
- be sensitive to the concerns of the taxpayers who support us.
- use only legal versions of copyrighted software in compliance with vendor license requirements.
- be considerate in your use of shared resources. Refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, connect time, disk space, printer paper, manuals, or other resources.
- individual end users are responsible for ensuring their operating system and anti-virus software is updated and that a college provided anti-virus program is periodically run to protect their desktop/laptop from infection.

In making acceptable use of resources you must NOT:

- use College resources to access obscene sites; these are off limits.
- use another person's system, login, password, files, or data or share your password with another person.
- use computer programs to decode passwords or access control information.
- download or display obscene material.
- circumvent or subvert or attempt to circumvent or subvert system or network security measures.
- engage in any activity that might be harmful to systems or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- use College systems for commercial, personal or partisan political purposes, such as using electronic mail to

circulate advertising for products, for political candidates or for any profit-making company, an enterprise or yourself.

- make or use illegal copies of copyrighted software, store such copies on College systems, or transmit them over College networks.
- download any on-line software without authorization of the Director of IT Services or the Chief Information Officer.
- use the network for purposes that place a heavy load on scarce resources (e.g., dial-in phone lines).
- no member of the community may, under any circumstances, use Holyoke Community College's computers or networks to libel, slander, or harass any other person. The following shall constitute Computer Harassment: (1) Intentionally using the computer to annoy, harass, terrify, intimidate, threaten, offend or bother another person by conveying obscene language, pictures, or other materials or threats of bodily harm to the recipient or the recipient's immediate family; (2) intentionally using the computer to contact another person repeatedly with the intent to annoy, harass, or bother, whether or not any actual message is communicated, and/or where no purpose of legitimate communication exists, and where the recipient has expressed a desire for the communication to cease; (3) intentionally using the computer to contact another person repeatedly regarding a matter for which one does not have a legal right to communicate, once the recipient has provided reasonable notice that he or she desires such communication to cease (such as debt collection); (4) intentionally using the computer to disrupt or damage the academic research, administrative, or related pursuits of another; (5) intentionally using the computer to invade the privacy, academic or otherwise, of another or the threatened invasion of privacy of another.
- waste computing resources, for example, by intentionally placing a program in an endless loop or by printing excessive amounts of paper.
- use the College's systems or networks for personal gain; for example, by selling access to your login or to College systems or networks, or by performing work for profit with College resources in a manner not authorized by the College.
- use the College's systems or networks to transmit any material in violation of United States or Massachusetts laws or regulations.
- engage in any other activity that does not comply with the General Principles presented above.

Enforcement

College officials will review alleged violations of Acceptable Use policies on a case-by- case basis. Violations of policy will result in appropriate action, such as: loss of electronic mail privilege, loss of computer privilege, consideration of appropriate disciplinary measures and/or referral to appropriate authorities responsible for enforcing state and federal laws concerning computer use.

Users who breach this code of practice may, after due process, be refused access to the College's computer and communications networks and may be subject to further disciplinary action. In an emergency, in order to prevent further possible unauthorized activity, the College may temporarily disconnect that user from the network. If this is deemed necessary by College staff, every effort will be made to inform the user prior to being disconnected, and every effort will be made to re-establish the connection as soon as the College determines it is appropriate.

The College considers any violation of acceptable use principles or guidelines to be a serious offense and reserves the right to copy and examine any files or information residing on College systems allegedly related to unacceptable use. Violators are subject to disciplinary action as prescribed in student and employee policies, handbooks, or contracts. Offenders also may be prosecuted under laws including (but not limited to) the Privacy Protection Act of 1974, The Computer Fraud and Abuse Act of 1986, The Computer Virus Eradication Act of 1989, Interstate Transportation of Stolen Property, Family Educational Rights and Privacy Act (20 U.S.C. Section 1223g), Massachusetts Wiretap Statute (G>L. c.272, Section 99), Massachusetts Privacy Statute (G.L. c. 214, Section 1B), Copyright Infringement laws (17 U.S.C. Section 101 et seq.), the Communications Decency Act of 1996 (47 U.S.C. Section 223 (d) - (h))and the Electronic Communications

Privacy Act of 1986 (18 U.S.C. Sections 2510-21, 2701-10,3121-27). Access to the text of these laws is available through the Reference Department of the Library of Holyoke Community College.

If you have reason to believe that this policy is being violated, you should report it as follows:

- Student violations to the Vice-President for Student Affairs
- Staff violations to the Vice-President for Administration & Finance
- Faculty violations to the Vice-President for Academic Affairs

2. Use Priority

While supporting the general principle of open and universal student access, eligibility for systems access will be determined by the following priorities if insufficient resources are available:

The highest priority is awarded to students where network access is a mandatory requirement of a course in which they are currently enrolled.

- At the next level, access will be granted where there is a demonstrated, but non-mandatory requirement for network access as described in a course guide.
- The lowest or non-essential level of access will be based upon the general principle of universal access and support for academic pursuit while not directly stipulated within a prescribed course of study.

3. Privacy

Computers owned by the College are provided for business and educational use only. Note that the College retains ownership of all communications as business records and these records may be subject to discovery in litigation. Any information on a College computer may be subject to the state's public records law and may therefore be subject to disclosure on request. By using computers on campus, employees are waiving their right to privacy and are consenting to College review and monitoring of communication and of their computer use. The College does not routinely monitor computer files or content unless it has received notice of possible misuse, security incident or violation of policy.

But in the course of routine maintenance, the content of your computer files may become visible and an apparent violation may be reviewed. The authorization to review files and computer logs rest with the president, who may delegate this responsibility to the CIO or Chief Financial Officer.

Private communications across the College's data networks will have the same protection as private communications via telephone. Unauthorized interception, reading, copying or modifying of private electronic data by a student or an employee will be in breach of this policy and subject to disciplinary or legal proceedings. The College will not guarantee this privacy as a result of routine maintenance, technical fault or criminal activity. See also comments under the Electronic Mail Policy; note that any electronic mail message may be forwarded by the recipient or printed and distributed. The privacy of e-mail, therefore, cannot be guaranteed.

Further:

Except in the course of investigation of an alleged violation of policy or a security incident, no College employee will be permitted to intercept, read, copy or modify private electronic data (either in transit across a network or stored within a computer system) without the written consent of the President or the consent of the addressee or sender.

While the College will endeavor to maintain the privacy of personal communications, it will monitor traffic load, and where necessary, take action to protect the integrity and operation of its networks.

Further the College will:

Collect utilization statistics based upon network address, network protocol and application use.

Progressively restrict non-essential users where network utilization results in performance degradation. Such restriction will be publicized to users through appropriate means.

4. Security

The College does not permit the transfer of logins and passwords between authorized and non-authorized persons. Such action is deemed unacceptable and will be the subject of disciplinary action.

Further:

Persons requiring systems access may not borrow another person's login. That person must request his/her own login from the appropriate staff member i.e. Product Manager, CIO or Vice President.

If it is necessary to allow an authorized third person to access a user's files or data, as in the case of illness or changing of positions, this information will be transferred by the system administrator rather than via the transfer of the login and password, Banner users will contact their respective Product Manager, Network and email accounts are administered by ITD.

Student user accounts will be disabled one academic year after a Student has graduated or one year after the last registered class.

Staff user accounts will be disabled following the termination of employment or when no longer under contract.

Banner security and password protection is the responsibility of the respective supervisor and the individual end user. Each supervisor, working through their respective product manager and vice president will initiate training that will result in password authorization and issue orders for password revocation. Revocation can be for cause or at the end of employment and is processed through the Banner Product Manager.

5. Eligibility for and Cost of Accounts

The following persons are eligible to hold accounts on the College computer network:

- All registered students (credit and non-credit)
- Employees (full or part-time)
- Members of the Board of Trustees (as space allows)
- Members of the Board of Directors of the HCC Foundation (as space allows)
- Retired employees of the College (as space allows and with consent of HR)
- Guests/Visitors using campus resources

Holyoke Community College owns all computer accounts and grants to the user the privilege of using such accounts. There is no cost for computer accounts, but file space will be limited for all users.

6. Electronic Mail Policy

General:

Electronic mail (email) is an official method of communication at the college, delivering information in a convenient, timely, cost-effective and environmentally sensitive manner. Printing and manual distribution of emails is highly discouraged and cost prohibitive.

It is the policy of this institution that:

All staff, faculty, students and applicable personnel have access to email, and the College may send official communications via email and electronic mailing lists.

Privacy Issues:

While email is personalized and relatively confidential, there is no guarantee of absolute privacy in a computer system. Computer users should be aware that state law applies to records stored in computers as well as on paper. Recent rulings indicate that the public has a right to review any documents created on email

by government officials and that companies who own the media on which email is implemented have the right to read that email. Federal and state law may require the College to examine email under some circumstances including provision of messages to outside agencies. However, employees of Information Technology Division at the College are prohibited from accessing information for which they have no job-related "need to know." They are also expected to maintain the strictest confidentiality regarding any information obtained during the course of fulfilling their job function.

Appropriate Use of Email:

Use of electronic mail is to be consistent with the Acceptable Use Policy of Holyoke Community College. Use of HCC computers for electronic mail that is not consistent with our Acceptable Use Policy may result in termination of electronic mail privileges. Electronic mail should be used as a source of information and efficient communication by students, faculty and staff.

Guidelines - Sending Messages:

- Create single subject messages whenever possible.
- Exercise caution. The confidentiality of your message cannot be guaranteed. Messages can be misdirected and/or be forwarded by recipients to other electronic mail addresses.
- Because messages can be saved on storage media or be forwarded to recipients at other electronic mail addresses, assume that any message you send is permanent.
- Separate opinion from non-opinion and clearly label each.
- If emotion is included in a message, clearly label it.
- Identify yourself clearly.
- Be selective in sending messages to listserves, interest groups, bulletin boards, etc.
- Do not insult or criticize third parties without giving them a chance to respond.
- Avoid large or multiple attachments.

Receiving Messages:

- If you receive a message intended for another person, notify the sender.
- Avoid responding while emotional.
- If a message generates emotion, look again.
- Avoid signing up for unnecessary outside newsletters or distribution lists using our HCC email address.

Spoofing, Phishing and Spear Phishing

Spoofing is when a user impersonates another device or user in order to steal data, spread malware, or bypass access controls. Phishing is the fraudulent attempt to obtain sensitive information such as usernames, passwords, Social Security numbers, credit card numbers or other Personally Identifiable Information (PII), by disguising oneself (spoofing) as a trustworthy entity in an email. Spear phishing is a form of phishing that targets an individual or business by using publically available information from social media or a company website.

These and other scams use social engineering techniques to persuade a target into providing information or performing an action that would not otherwise be provided or done.

Social engineering techniques include the use of urgent language and threat of consequences, such as your account will be disabled if you do not verify it now. This includes a short timeframe for action to prevent thinking about the situation.

HCC ITD will never ask for your password or have you verify your password via email. You verify your account every time you log in.

7. Use of Copyrighted Materials

The College recognizes that accomplishment of its mission may be facilitated by the use of works owned or created by others. All faculty, staff and students shall recognize those accomplishments by respecting the intellectual property of others and using such works only to the extent such use is permitted by law.

This policy shall apply to students, employees, and other individuals who use College equipment and/or facilities and to students, employees, and other individuals who use off-campus non-College facilities and/or equipment in connection with College related activities or on behalf of the College. For example, this policy applies when photocopying is undertaken at a commercial copying center, at a self-service coin-operated machine in the library, or on any other reproduction equipment owned or leased by the College or used in connection with College activities or on behalf of the College.

Employees and other individuals subject to this policy who use material originated by others shall not, as a matter of policy, when using such materials, infringe on those rights of the originator which are protected by copyright laws and shall secure permission to use or reproduce copyrighted works when such permission is required under copyright law and/or pay royalties when such payment would be required. Employees and other individuals subject to this policy are expected to obtain permission from the copyright owners unless the intended use is clearly permitted under the doctrine of "fair use."

"Fair Use" shall not be abused. The College will not tolerate copying instead of purchasing copyrighted works where such copying would constitute copyright infringement.

For purposes of this policy copyrighted material means any work or intellectual property which may be subject to copyright under the laws of the United States. This includes but is not limited to literary works, including computer programs and compilations; musical works, including any accompanying words; dramatic works, including any accompanying music; pantomimes and choreographic works; pictorial, graphic, and sculptural works; motion pictures and other audiovisual works and sound recordings. For example, this policy applies to photocopying for classroom use, use of computer software, use of videocassettes, and off-air videotaping, CD's, DVD's or other media types.

This policy is not intended to waive any rights, remedies, immunities or defenses available to the College in the event of an infringement or alleged infringement of the copyright law and such rights, remedies, immunities and defenses are specifically reserved.

8. Password Policy

General Policy Provisions:

Passwords are an essential aspect of computer security, providing important front-line protection for electronic resources by preventing unauthorized access. Passwords help the college limit unauthorized or inappropriate access to various resources at HCC, including user-level accounts, web accounts, email accounts, screen saver protection, and local router logins as well as Banner accounts.

A poorly chosen password may result in the compromise of HCC systems, data or network. Therefore, all HCC faculty and staff are responsible for taking the appropriate steps, as outlined below, to select appropriate passwords and protect them. Contractors and vendors with access to HCC systems also are expected to observe these requirements.

A department and/or system administrator may implement a more restrictive policy on local systems where deemed appropriate or necessary for the security of electronic information resources. The Information Technology Division or Banner Product Managers can require a more restrictive policy in protection of confidential data.

Creation of Passwords for HCC related systems

Passwords created by users of college systems, should conform to the following guidelines:

- Must be different than the user's login name or the reverse of the name and must avoid use of knowable personal information (names of family, etc.).
- Must be a minimum of 8 characters.

- Must contain at least one capital letter, one lowercase letter, one number and/or special character or symbol.
- It CANNOT contain part of the username.

These provisions will be enforced electronically whenever possible.

Changing passwords

Passwords for network access, Email, Moodle, Rave, and Online Services will be changed every 180 days and Banner passwords every 90 days. These changes will be forced by the respective systems administrator. The new password must differ from the old password by at least three characters.

Protecting a password

- Passwords should be treated as confidential information.
- Passwords should never be written down or posted for reference.
- Passwords should not be included in email messages or other forms of electronic communication.

Sharing a password

- Sharing or allowing another person to use an individual account password is a violation of this policy, unless the person is an information technology professional assisting you with a technical problem. Departmental account passwords should be shared only with appropriate departmental personnel.
- It is recommended that passwords be changed after allowing use as permitted in this section.
- Approval of ITD is required prior to sharing a password with a vendor (approval may be granted on a one-time or continuing basis), and this vendor access may require implementing the appropriate technology infrastructure to accommodate the access (depending on the circumstance, and as determined by ITD). Vendors or consultants accessing HCC systems should be made aware of this Acceptable Use Policy.

Reporting a password compromise

- Suspected compromises of passwords must be reported immediately to the Help Desk at x2075
- The password in question should be changed immediately.

Responsibilities of Information Technology Division

ITD may require a more restrictive policy, such as stronger passwords, in some circumstances.

ITD or its delegates will perform regular security scans for violations of acceptable use or breeches of security.

In the event of a suspected security issue or account compromise, ITD may need to reset the password to gain access to the account for analysis or to disable the account altogether. Any action taken on the part of ITD will be only to safeguard the integrity and security of the HCC systems. ITD strives to maintain the highest level of confidentiality and privacy in regards to anything discovered during the course of an investigation that is unrelated to the acceptable use of HCC systems.

Consequences

Any individual who violates this policy may lose computer or network access privileges and may be subject to disciplinary action in accordance with acceptable use policy of the college, which may result in a range of sanctions up to and including suspension or dismissal for repeated or serious infractions.