Bunker Hill Community College

Student Computer and Network Usage Policy

General Principles

Access to computer systems and networks owned or operated by Bunker Hill Community College imposes certain responsibilities and obligations and is granted subject to college policies, and local, state and federal laws. Acceptable use is always 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 individual rights to privacy.

Use of the Internet or World Wide Web must be consistent with the Student Computer and Network Usage Policy of Bunker Hill Community College. The college does not control, monitor, or restrict content accessed over the Internet or World Wide Web. Users are solely responsible for all materials viewed, stored, transmitted, or downloaded. Complaints or evidence of inappropriate use of the Internet or World Wide Web will be investigated and, if confirmed, may result in disciplinary action up to and including dismissal.

Eligibility for and Cost of Accounts

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

- Employees (full or part-time)
- Currently enrolled BHCC students
- Others as designated by the President or the President's designee

Bunker Hill Community College owns all computer accounts and grants to the user the privilege of using the resources. File space will be limited for all users. Students may access computer resources, including the Internet and the World Wide Web, at no charge, from campus based machines. No remote access to the college network is provided to students at this time.

Passwords

Passwords should be selected so that someone close to you does not easily guess them. For example, do not use your pet's name, your birth date, favorite car, etc. Furthermore, passwords should not be dictionary words because they also are easily cracked. Passwords should be at least eight characters long and contain a combination of letters, numbers and special characters. For example, "Pa55w0rD" Passwords should be reset every six months and not written down where they may be discovered and used by someone else.

Use Priority

While supporting the general principle of open and universal student access, eligibility for service will be determined by the Chief Information Officer, or designee, using the following priorities, if insufficient resources are available:

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

The next level priority will be granted where there is a demonstrated, but non-mandatory course requirement for computer use as described in a course syllabus or 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.

Guidelines

In making acceptable use of resources students must:

- Use the College's Web Site, Server, and all other related computer equipment and services only for academic, educational, or professional purposes, which are directly related to official College business and in support of the college's mission.
- Be responsible for all activities conducted using your BHCC user IDs.
- Not disclose their user BHCC IDs to anyone.
- Access only BHCC files and data that are your own, that are publicly available, or to which you have authorized access.
- Be considerate in your use of shared resources and refrain from monopolizing systems, overloading networks with excessive data, or wasting computer time, disk space, printer paper, manuals or other resources.
- If it is necessary to allow an authorized third person to access a user’s files or data, as in the case of illness, a formal request must be made in writing to the appropriate Academic Dean or Dean of Student Affairs. In this case, the information will be transferred to the third party by the system administrator rather than via the transfer of user ID and password.
- Student user accounts and all data found in student user accounts may be removed at the end of each semester.

The following are prohibited:

- Use of another person's user ID or password.
- Use of another person's files or data without permission.
- Unauthorized interception, reading, copying or modifying of private electronic data.
- Use of computer programs to decode passwords or access controlled information.

- To view, download, store, or transmit obscene materials, including but not limited to nudity, child pornography, or violent materials or material that threatens the public safety or safety of individuals. Materials are considered obscene if: (1) the average person, applying community standards, would find the material appeals to the prurient interest: (2) the material describes and depicts sexual conduct in a patently offensive manner; and (3) taken as a whole, the material lacks serious academic, literary, artistic, political or scientific value.
- To circumvent, subvert, or attempt to circumvent or subvert system or network security measures.
- To purposely engage in any activity that might be harmful to system/network or to any information stored thereon, such as creating or propagating viruses, disrupting services, or damaging files.
- Pursuant to Massachusetts Campaign Finance Laws, no governmental resources (including computers, networks, fax machines, modems, printers, and/or copy machines) may be used by any person in order to promote or oppose a political candidate or ballot question or for the purpose of disseminating materials that advocate a particular vote on a ballot question or a political candidate. This would include making or using illegal copies of copyrighted software, store such copies on College systems, or transmit them over College networks.
- To download any on-line software without authorization from the Chief Information Officer or his/her designee.
- To use the network for purposes that place a heavy load on scarce resources.
- To use Bunker Hill Community College's computers or networks to libel, slander, or harass any other person. The following shall constitute Computer Harassment: (1) 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) Using the computer to contact another person repeatedly once the recipient has provided reasonable notice that he or she desires such communication to cease; (3) Using the computer to disrupt or damage the academic research, administrative, or related pursuits of another; (4) Using the computer to invade the privacy, academic or otherwise, of another or threatened invasion of privacy of another.
- To waste computer resources, for example, by intentionally placing a program in an endless loop or by printing excessive amounts of paper.
- To use the College's systems or networks for personal gain; for example, by selling access to your user ID or to College systems or networks, or by performing work for profit with College resources in a manner not authorized by the College.
- To use the College's systems or networks to transmit any material in violation of United States or Massachusetts laws or regulations.
- To engage in recreational game playing.
- To engage in any other activity that does not comply with these Guidelines presented above.

Privacy

Users of the College's Computer Network System should have no expectation of privacy over any content, communications, transmissions, or work performed thereon. Computers owned by the College are provided for college and educational use only. Note that the college retains ownership of all computer transactions as business records and these records may be subject to discovery in litigation. Any information on a college computer or storage media may be subject to the state's public record law and may therefore be subject to disclosure upon request.

The College does not routinely monitor students' computer activities unless it receives notice of possible misuse or violation of policy. However, should the college discover, as a result of routine maintenance, technical fault or investigation of criminal activity, misuse or violation of policy, it will not guarantee privacy. By using computers on campus, students are waiving their right to privacy and are consenting to College review and monitoring of their computer use. Further:

- The College endeavors to maintain the privacy of personal communications. Where necessary, the college will take action to protect the integrity and operation of its networks.

- In the course of routine system maintenance, technical problems, investigation of an alleged violation of policy, or criminal investigations, college employees will be permitted to intercept, read, copy or modify private electronic data, either in transit across a network or stored within a computer system.

- The College will collect utilization statistics based upon network protocol and application use.

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

Additional General Principles and Guidelines for Electronic Mail

General Principles:

Students in the educational community should use electronic mail as a source of information and efficient communication. Use of electronic mail is to be consistent with the Student Computer and Network Usage Policy of Bunker Hill Community College. Use of BHCC computers for electronic mail that is not consistent with the Policy may result in termination of electronic mail privileges, sanctions as noted in the Student Disciplinary Policy, including dismissal, and prosecution by state and/or federal authorities.

Users of the College's Computer Network System for electronic mail purposes have no expectation of privacy over any email communications or transmissions sent or received. Further, the College may access email communications or transmissions for routine system maintenance, technical problems or in the investigation of criminal investigations.

Guidelines

Student e-mail accounts will have limited storage for messages sent or received. If students' intend to save e-mail messages, they must remove messages from the system upon sending or receiving them (i.e. by print or archive).
Sending Messages:

- Create single subject messages whenever possible.
- Do not send or forward chain letters.
- 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 without your knowledge.
- 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. It is difficult to convey emotional content without the benefit of body language or tone, resulting in the misinterpretation of your message.
- Identify yourself clearly.
- Before sending messages to list servers, interest groups, bulletin boards, etc., be sure the message is appropriate for the entire group.

Receiving Messages:

- If you receive a message intended for another person, notify sender.
- Avoid responding while emotional.
- Consider alternative media.

Enforcement

All alleged breaches of the Student Computer and Network Use Policy will be referred to, reviewed, and addressed by the appropriate college official(s) and subject to provisions of the Student Disciplinary Policy & Procedures, Handbooks or Contracts.

Offenders may also be referred to state or local authorities for potential violation of the following (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 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 sq.)
- The Communications Decency Act of 1996 {47 U.S. C. Section 223 (d) MN (ah)]
- The Electronic Communications Privacy Act of 1986 (18 U.S. C. Sections 2510-21, 2701-10, 3121-27)
- The Family Educational Rights and Privacy Act (FERPA)
- Massachusetts Defamation laws
- State and Federal sexual harassment and discrimination laws

Access to the text of these laws is available through the Reference Department at the Library of Bunker Hill Community College.