Acceptable Use of Information Technology Policy

Bergen Community College reserves the right to monitor its information technology resources and telecommunications network to protect the integrity of its computing systems, workstations, and lab facilities, and to ensure compliance with all acceptable use and related policies and procedures. To this end, the College reserves the right to inspect any and all computer systems or data that reside on its telecommunications network for violations of any acceptable use and related policies and procedures.

I. Acceptable and Unacceptable Use

Because of the richness of the Internet and the College's information technology resources, it is not possible to catalogue exhaustively all acceptable and unacceptable uses. The lists below are meant to be illustrative. Employees and students should consult with their supervisors or classroom instructors, respectively, about the appropriateness of other uses. In free time areas, users should address questions to lab supervisors or other responsible parties.

In deciding what is and is not an acceptable use, there are two overriding principles: (1) the College's information technology and telecommunication resources exist to support the College's mission, and (2) the College is committed to ensuring a positive learning environment for all members of its community. Thus, all users are obliged to demonstrate civility in any and all exchanges and postings, including the content of web pages, both official and unofficial. The College reserves the right to remove from its telecommunications networks any content judged to be racist, pornographic, or designed to denigrate members of the College community.

a. Acceptable Use

1. Gathering and providing research material and data
2. Analyzing research data
3. Preparing course materials
4. Completing class and homework assignments
5. Enhancing coursework
6. Enhancing educational approaches and teaching methods
7. Obtaining and disseminating college related knowledge
8. Developing and administering targeted demographic surveys
9. Using WebAdvisor to register online for courses or to access information about one's own academic performance

10. Using Datatel’s Colleague or other institutional software within the scope of one’s normal duties.

b. Unacceptable Use

1. Using the network for gambling, any other illegal activity, or any activity prohibited by the College’s acceptable use and related policies and procedures, including but not limited to violations of copyrights, software agreements and other contracts
2. Using the College systems for commercial or profit making purposes
3. Altering system or software or hacking in any form
4. Gaining unauthorized access to resource entities, including use of others’ passwords
5. Invading the privacy of individuals
6. Posting anonymous messages
7. Creating and displaying threatening, obscene, racist, sexist, or harassing material including broadcasting unsolicited messages or sending unwanted mail
8. Disobeying lab and system policies, procedures, and protocols (e.g., time limits on workstation usage)
9. Using the network in support of groups outside the College when such use is not in keeping with the mission of the College
10. Creating and using individual web pages not primarily focused on the mission of the College
11. Using WebAdvisor to access information about someone other than oneself
12. Accessing data or making use of data in Datatel’s Colleague or other administrative systems software not relevant to the scope of one’s job responsibilities.

II. Privacy and Use of Information

Employees are expected to be knowledgeable of, and to perform their duties in compliance with, federal, state, and local laws and College policies, including the provisions of the Family Educational Rights and Privacy Act designed to protect the confidentiality of data and the privacy of individuals. Employees are expected to attempt to access, through any system, only information that is needed in the context of the performance of their normal duties and to exercise good judgment in the use of such information. In particular, confidential or demographic data, which pertains to students, employees, or College operations, must be used in a manner that protects rights of privacy and limits personal and institutional liability. In general, employees are expected to avoid situations in which they either provide or interpret others’ information which is outside the scope of their expertise or job responsibilities. Please consult the Manager of Training and Compliance for further clarification of compliance issues.

III. Security Breaches

Attempts to alter system software, to bypass security protocols, to introduce viruses, worms, or other malicious or destructive programs, or otherwise “to hack” are expressly forbidden. Any member of the College community, including a student, who intentionally breaches security will be subject to disciplinary action, including suspension and dismissal.

IV. Incidental Personal Use

Incidental personal use is an accepted and appropriate benefit of being associated with Bergen Community College’s rich technology environment. However, this type of personal use must still adhere to all College appropriate use and related policies and procedures, and must never have an adverse impact on uses of technology and information resources in support of the College’s mission. The College Administration reserves the right to define the acceptable level of personal incidental use. An employee’s supervisor may also decide that personal activities are affecting the abilities of the employee or colleagues to perform job functions, and it is his or her right to require the employee to cease those activities.

V. E-mail

E-mail is defined as all technologies used to transfer messages, including e-mail, instant messaging, and peer to peer file exchange. E-mail is a tool for business purposes. Users have a responsibility to use this resource in an efficient, effective, ethical and lawful manner. In general, e-mail communications should follow the same standards expected in written business communications and public meetings.

a. Accounts

It is the intention of the College to have on file email addresses for all full time faculty, administrators, adjuncts, and students. Email accounts are also provided for staff whose job responsibilities include regular computer access. Generally, email accounts are closed when employment ends. However, the College may choose to extend email privileges to adjuncts during periods of stop-out. Further, upon request, the College will keep active email accounts for Professor Emeriti and retired full-time faculty.

1. Full-Time Employees

In the case of full-time employees, addresses using the Bergen domain will be assigned. The College will use these addresses in all email communication with full-time employees. Full-time employees are expected to check their email daily during their work week.

2. Part-Time Employees

In the case of part-time employees, addresses using the Bergen domain will be assigned when required to perform the assigned job function. Part-time employees are expected to check their email daily during their work days.

3. Adjunct Faculty

For adjuncts, the College will supply an address with a Bergen domain, if requested or if no email address is available in Colleague. These addresses may be requested by contacting the BCC Help Desk. Adjuncts must supply appropriate College identification to receive an account. Alternatively, adjuncts may use WebAdvisor to supply a preferred (non-BCC domain) address. If so, the College will use this address for all email communications. Adjunct faculty are expected to check email at least once a week. The College will not maintain more than one email address for any faculty member.

4. Students

All students enrolled in credit courses are required to have a valid email address on file in Colleague. Students may enter a preferred email address in Colleague using WebAdvisor.

b. Broadcast Email to Employees

Authority to use the entire master list of email addresses of College employees rests with the Executive Staff. System-wide electronic messages should be used sparingly for urgent, emergency notices, such as Public Safety announcements and other matters affecting the entire campus community. The frequency, content, and other characteristics of most messages are inappropriate for such wholesale delivery. In particular, it is not appropriate to use system-wide email broadcasts to publicize college events which are not of an urgent nature or of primary interest to all members of the college community. In these instances, departments may wish to announce such events on their departmental website or on the College-wide Outlook Bulletin Board. Email server groups may be set up to allow targeted distribution of email, such as to the members of an academic division. Further, end users may create their own personal distribution lists. However, users should take care not to broadcast unwanted email messages. Requests to be removed from personal distribution lists must be honored.

c. Colleague Broadcast Email to Students

Authority to send email to all students using the Colleague system rests with the Administrative Vice President and the Vice President of Student Services. In cases of emergency, the Office the the Director of Technologies may be contacted. Such email is strictly limited to the official conduct of College business, and is not to be used for promotion or marketing purposes. All Colleague broadcast email must include the following footer: "You have received this email because you are or have been a student at Bergen Community College. If you do not wish to be contacted by email, please reply to noemail@bergen.edu."

Student Clubs and other groups wishing to use email to promote events or other activities should maintain separate distribution lists, targeting only those who have indicated interest in receiving such communication.

d. Strictly Prohibited

The following use of e-mail is strictly prohibited. Employees receiving such material should immediately report it to their supervisors.

- The creation and exchange of messages that are offensive, harassing, obscene or threatening
- The exchange of privileged, confidential or sensitive information to inappropriate persons
- The creation and exchange of advertisements, solicitations, chain letters, or other spam
- E-mail use for commercial purposes
- The creation, storage or exchange of information in violation of copyright laws
- Reading or sending messages from another person's account, except under proper delegate arrangements
- Copying or forwarding messages belonging to another user which have been altered in such a way as to change the intent of the author.

e. Guidelines

Users should follow these guidelines and conventions:

- Ensure that messages are addressed to the appropriate recipient(s).
- Do not subscribe to list servers or other distribution lists that are *not* College related. Such lists tend to overload and affect the performance of the email system.
- Users must not compromise the privacy of their passwords by giving them to others or exposing them to public view. Passwords should be changed on a regular basis.
- Retain messages only if relevant to the work or an anticipated litigation. The College's e-mail system is set to retain messages for no more than six months. Messages having a legitimate business purpose greater than six months should be archived to a desktop folder or printed and filed.

- Address messages to recipients who “need to know”. Messages and attachments can carry viruses, and instant messaging (IM) and peer to peer technologies are often used by intruders with malicious intent.
- Avoid opening messages or attachments received from unknown senders or responding to instant messages or other peer to peer technologies from strangers. Messages and attachments can carry viruses, and instant messaging (IM) and peer to peer technologies are often used by intruders with malicious intent.
- Construct messages professionally (spelling and grammar) and efficiently (subject field, attachments).

VI. Colleague Access

College employees will be given access to the College’s administrative systems on an as needed basis. Accounts and security clearance must be authorized by the employee’s Executive Council member.

VII. Account Log-ons and Passwords

Account log-ons and passwords, including e-mail, are issued to individuals for their sole use and are non-transferable. Owners are responsible for all usage of their assigned accounts, log-ons, and passwords.

VIII. Violations of Acceptable Use and Related Policies and Procedures

Users are expected to notify the Office of Information Technology, classroom instructor, free time lab supervisor, or other responsible party, as appropriate, of intentional or unintentional breaches in access and data security of which they become aware. In addition, employees who are aware of serious violations of acceptable use or related policies and procedures (including malicious tampering, virus infection, or “hacking”) are required to report such activity to their immediate supervisors. In the case of complaints about materials believed to be offensive or otherwise inappropriate, users are encouraged to express their concerns directly to those believed to be misusing the systems and/or to lab supervisors. If the situation persists they should bring the matter to the attention of Public Safety or other responsible parties. Individuals who violate acceptable use and related policies and procedures will be subject to appropriate sanctions, including suspension, dismissal, and legal proceedings.

According to the U.S. Copyright Act, illegal reproduction of software or other material is an offense which will subject the violating individual to civil and monetary damages. The use of email or any College system for harassment or criminal activity may result in criminal penalties, including fines and imprisonment.