

Technology Usage Policy for EICCD

This policy applies to Eastern Iowa Community College District (hereafter referred to as "EICCD") which includes Clinton (CCC), Muscatine (MCC), and Scott Community Colleges (SCC). Technology resources and usage may be described as all EICCD-owned print and electronic media and services including, but not limited to: computers, EICCD phones (wireless or wired), printers, modems, email communications, EICCD web content, wireless connections, and fax transmissions. Personal equipment connected to the EICCD network is also subject to this policy.

As a public learning institution financed and supported by public funds, it is incumbent upon EICCD to ensure that its technology resources are responsibly and effectively maintained and used by all persons affiliated with EICCD. Such persons include credit and noncredit EICCD students, faculty, staff, student employees, alumni, EICCD, CCC, MCC, and SCC foundation participants, and guests at the institution who will be referred to throughout this procedure as EICCD technology users—or simply "users." The use of technology and information resources is governed by all applicable EICCD faculty, staff, and student policies as well as applicable federal, state, and local laws and statutes.

Students have 150 MB storage space (may vary depending on available resources) within CampusCruiser for emails and electronic files. CampusCruiser has a usage policy available by clicking on the "Campus" tab and then selecting "Terms of Usage" on the menu. Accounts that exceed this limit will be contacted by the EICCD CampusCruiser administrator and will be asked to take steps to return to the 150 MB limit. Accounts that are not returned to 150 MB by the stated date are subject to possible removal of data at the discretion of the EICCD CampusCruiser administrator.

Statement of General Expectations

All EICCD technology users must abide by applicable federal and state laws and regulations regarding technology usage, as well as existing District policies and procedures. Paramount to EICCD's mission as an institution of higher learning, EICCD values academic freedom and academic achievement. EICCD promotes openness to new ideas, sensitivity to multicultural issues, and unlimited access to a wide range of information and ideological perspectives. The District values the free flow of information and does not condone censorship.

Individual Responsibilities

Technology resources users are expected to:

- Use technology in a manner consistent with federal, state and local laws.
- Support an educational environment free from harassment and discrimination as described in the Employee and Student Handbook.
- Use technology resources appropriately so as to not interfere with the educational mission of the institution or the daily business of the District.
- Students and employees are expected to make backup copies of their work to ensure against loss.
- Use strong passwords and change them frequently.
- Be aware of and employ security practices to prevent unauthorized access to user computers, accounts, passwords, user names, and personal identification numbers (PIN). This would include logging off from the computer following usage, avoiding sharing PIN and other passwords, and using secure methods for sharing, storing or transferring information.
- Use technology resources consistent with other institutional policies.
- Assist in maintaining and enhancing the integrity of EICCD technology resources by taking measures to support the security and privacy of computer networks.

- Report any systems interference, technological performance problem, or damage to equipment to the Help Desk (336-3456 or helpdesk@eicc.edu) or the computer lab supervisor on duty.

Prohibited Conduct

- Disrupting access of students, faculty or staff members to technological resources.
- Obtaining or gaining unauthorized access to EICCD computer systems or an account for another individual. This includes the unauthorized access, willful damage, or misuse of systems, applications, databases, code, files, or data.
- Attempts to make unauthorized alterations or to cause interruptions of system configurations or programs that protect data or secure systems.
- "Computer hacking" (i.e. unwanted or unsolicited entry into a computer system). This includes, but is not limited to, successful acts of hacking, unsuccessful hacking attempts, possession of the tools used for computer hacking, or running programs that attempt to obtain passwords, codes, access files, or confidential data.
- Using technological equipment to interfere with the lawful rights of others by such activities as falsifying or altering records or software, creating fraudulent documents, damaging programs belonging to the EICCD or another individual.
- Knowingly introducing a "computer virus, worm, Trojan, malware or spam" to a computer or network (i.e. a program - either harmless or damaging - which attaches itself to another program and has the capability to reproduce in order to infect other computers).
- Sending harassing, threatening material, or information to another individual (as defined by the EICCD Harassment Policy).
- Violating license agreements, copyrights, or intellectual property rights including copyright, patents, etc., by copying, distributing, or publishing intellectual property. This includes the unauthorized copying of any software (including operating systems, programs, applications, databases, games, music, movies, videos, text, or code) which is licensed or protected by copyright.
- Permitting other persons—whether EICCD users or unauthorized users—to use a EICCD user's accounts, passwords or access codes or allowing others to use your personal username and password to access campus networks or other technology resources.
- Theft of EICCD hardware or software.
- Inappropriate or malicious use of technology resources including attempts to alter, erase, damage or intercept technological data or programs that are the property of EICCD or EICCD users.

Copyright

EICCD recognizes and adheres to the U.S. and International copyright laws, software licenses, and intellectual property rights associated with both print and non-print materials. EICCD forbids, under any circumstances, the unauthorized reproduction of software, use of illegally obtained software, or gathering or distribution of illegally obtained copyrighted digital materials. Using EICCD equipment for any of these purposes is prohibited. EICCD employees and students who violate this policy are subject to disciplinary action. Individuals who violate U.S. copyright law and software licensing agreements also may be subject to criminal or civil action by the owner of the copyright.

Distributing copyrighted songs, games, videos, movies, or other copyrighted files or materials without permission is a violation of the Federal copyright laws. Individuals who violate U.S. copyright law and software licensing agreements also may be subject to criminal or civil action by the owner of the copyright. EICCD will cooperate with any criminal investigation regarding these matters. According to copyright laws, you do not need to be making a profit to be prosecuted for distributing copyrighted materials such as music, movies, games, and software files.

Security and Privacy

Security of technology resources is of the utmost importance—all users are expected to cooperate in maintaining and enhancing the integrity of these resources. EICCD reserves the right to inspect or monitor technology resources under its control, and to take appropriate action when there is reason to believe that a user has violated established policies. Every effort shall be made to protect the Constitutional rights of all EICCD technology users.

EICCD does not endorse the casual review of electronic communication and storage. However, users should be aware that their uses of EICCD information technology shall have no guarantee of privacy. Technology resources are considered property of the EICCD and EICCD may initiate inspections or monitoring of information resources if it is deemed to be in the best interest of EICCD. EICCD may also be required to initiate inspections or monitoring if subject to subpoena or other legal requirements.

Staff Access to Institutional Data

The value of data as an institutional resource is increased through its widespread and appropriate use; its value is diminished through misuse, misinterpretation, or unnecessary restrictions to its use. Access to EICCD institutional data - the permission to view or query institutional data - should be granted to all eligible employees of EICCD for legitimate EICCD purposes. Network accounts (usernames) will be administered by EICCD Technology Information Services for all staff. Data users will be expected to access institutional data only in their conduct of EICCD business, to respect the confidentiality and privacy of individuals whose records they may access, to observe any ethical restrictions that may apply to data to which they have access, and to abide by applicable laws and policies with respect to access, use, or disclosure of information. Expressly forbidden is the disclosure of limited-access or internal institutional data or the distribution of such data in any medium except as required by an employee's job responsibilities.

Responsible Use

The user bears the primary responsibility for the material that he or she chooses to access, send, or display. Respect the rights of others by complying with all EICCD policies. Remember that you are representing EICCD in all of your communications. Use only computer IDs or accounts and communications facilities, which you are authorized to use, and use them for the purposes for which they were intended. Do not let others use your username or password.

Students will be responsible for maintaining their own files that are stored in CampusCruiser including deleting files no longer in use, and copying files that they want to save to removable media.

Employees will be responsible for maintaining their own files that are stored on network drives including deleting files no longer in use. Do not use up valuable network storage resources with unnecessary, personal files, and outdated files.

Internet and Email Use Policy

A separate Internet Use Policy provides specific policy statements concerning usage of the internet by employees and students as well as policies regarding email. This policy is located at http://www.eicc.edu/internal/district1/Internet_Use_Policy.doc.

Personal Use of EICCD Technology

Personal use of EICCD technology by all EICCD technology users must be viewed in the context of EICCD's academic mission. Usage preference shall be granted to users who are engaged in

academic or work-related activity (as opposed to recreational usage) and should adhere to the following guidelines:

Users engage in no activity that harms the performance of technology, damages or defaces equipment, or knowingly exceeds the design parameters of the equipment, building or work facility.

Priority in student computer labs is given to users for the completion of academic activities.

Access or use of any institutional data for one's own personal gain or profit, for the personal gain or profit of others, or for political purposes is strictly forbidden.

Enforcement of Technology Usage Policy

Interim Response: EICCD Information Technology personnel may temporarily disable an account or service to an individual when there is reason to believe an alleged violation of the Technology Usage Policy is believed to have occurred. This may happen when one of the alleged violations:

- Violates federal, state or local law;
- Could result in damage or interference with official EICCD business; or
- Could result in liability for EICCD.

Disciplinary Action: A student who is believed to have violated the Technology Usage Policy may be charged with a violation of student conduct as stated in the Student Handbook. An employee who is believed to have violated the Technology Usage Policy may be charged with a violation of the employee conduct stated in the Employee Handbook. Discipline and appeal processes will follow the established procedures in the respective Handbooks.

Employees will be asked to sign the "[Short Form E-mail and Computer Use Policy](http://www.eicc.edu/internal/district1/Short_Form_E-mail_Computer_Use_Poli.pdf)" located at http://www.eicc.edu/internal/district1/Short_Form_E-mail_Computer_Use_Poli.pdf