Appropriate Use of Information Technology Resources Policy *(*200.2)

Effective date: June 11, 1996
Revised: August 17, 2005
Revised: April 19, 2016
Revised: May 16, 2017
Revised: October 17, 2017
Revised: May 18, 2021

In pursuit of its mission to deliver exceptional education and services to improve the lives of our students and to strengthen our communities, the Board of Trustees of Illinois Eastern Community Colleges ("IECC" or the "District") provides access to “information technology resources” (as defined below) for students, employees and other constituents within institutional priorities and financial capabilities.

Access to District information technology resources may be granted by the data owners of that information based on their judgment of the following factors: relevant laws and contractual obligations, the requestor's need to have access to the information technology resources, the information technology and resources’ sensitivity and the risk of damage to or loss by the District which could result from its disclosure.

The District reserves the right to extend, limit, restrict or deny privileges and access to its information technology resources. Data owners--whether departments, units, students, or employees--may allow individuals other than District students or employees access to information which they own or for which they are responsible, so long as such access does not violate any license or contractual agreement, District policy or any federal, state, county or local law or ordinance.

IECC information technology resources are to be used for the District-related activities for which they are intended and authorized. District information technology resources are **not** to be used for commercial purposes or non-college related activities without written authorization from the District. In these cases, the District will require payment of appropriate fees. This policy applies equally to all District-owned or District-leased information technology resources.

All users of IECC's information technology resources must act responsibly in their use of the resources. All users of District-owned or District-leased information technology resources must respect the rights of other users and comply with all pertinent licenses and contractual agreements. IECC's policy requires that all students, employees, and other authorized users act in accordance with these responsibilities, relevant laws and contractual obligations and the highest standard of ethics. Each user must remember that his/her freedom to access, display or publish information is constrained by the rights of others who have the right not to be subjected to material that they find offensive. Information posted and/or published on the Internet may be accessible by any computer on the Internet.

Authorized users must all guard against abuses that disrupt or threaten the viability of any and all systems, including those at the college campuses and those on networks to which the District's systems are connected. Access to information technology resources without proper authorization from the data owner(s), unauthorized use of District computing facilities, and intentional or negligent corruption or misuse of information technology resources are direct violations of the District's standards for conduct as outlined in IECC Policies and Procedures, District collective bargaining agreement and the Faculty Handbook and may also be considered civil or criminal offenses.

Privacy and Content
Users should have no expectation of privacy or confidentiality in the content of electronic communications or other computer files sent and received on the District computer network or stored on any IECC information technology resources. The District Information Technology Department Staff, College Technicians, or other District employees, may, at any time, review the subject, content, and

appropriateness of electronic communications or other computer files, and remove them if warranted, reporting any violation of rules to the District administration and/or law enforcement officials.

Account Security and Information Exchange
User IDs and passwords are provided for technology systems and are only for individual use. Users should not share passwords with anyone and should not use anyone else's password regardless of how the password was obtained. If a user suspects someone has discovered his or her password, the password should be changed immediately and the IT Help Desk should be notified. Users shall not intentionally modify files, data, or passwords belonging to other users. When sending electronic communications, users should be cautious when including personal information. IECC is not responsible for personal information which is obtained by unauthorized recipients or interceptors of electronic communications. Use of personal credit cards on an IECC owned computer is done at the user's own risk and IECC is not responsible for any loss or damages resulting from this use.

Multi-factor Authentication
Multi-factor authentication (MFA) is also required for all users accessing IECC's systems. MFA is a method of computer access control in which a user is granted access only after successfully presenting multiple separate pieces of evidence to an authentication mechanism – typically at least two of the following categories: knowledge (something they know), possession (something they have), and inherence (something they are). IECC utilizes four MFA verification methods: 1. The Microsoft Authentication App, 2. A text message to a cell phone, 3. A phone call to any 10-digit phone number, 4. A digital token key. Digital token keys will be available on a case-by-case basis. A lost or stolen MFA token should be reported immediately to the IT Help Desk. A replacement charge of $25.00 may be applied for any lost or stolen token.

Employee Account Setup Process
Each IECC location has designated employees (President/Dean offices or other administration) that may request accounts for employees by completing the Information Technology Services Request Form. This form is submitted to the Human Resources and Information Technology Departments for verification and processing. When the accounts have been created, the Information Technology Department sends account information to the employee via email, text, or mail. Banner system accounts also require the completion of the Banner Security Request form. MyIECC account details are also included with the IT Services Request that allow employees and faculty access to various course and employee resources.

Student Account Setup Process
Student accounts are generated during the application acceptance process. Credentials are sent to a student by encrypted email to setup their MyIECC account. Student Services in some cases may directly issue credentials to create an account using a GeneratedID and PIN. In either process the student must complete account setup and set a new password. Students may be required to use multi-factor authentication for additional account security. (See MFA section of this document). The MyIECC account provides access to many services including email, online courses, electronic course materials, schedules, grades, tax forms, account balances, emergency alerts, library service, and much more.

Student Email and Electronic Communications
IECC provides email accounts to students as a tool for sharing important and official information regarding registration, financial aid, deadlines, student life, and more. Email allows IECC to communicate quickly and efficiently and provides standardized, consistent communication with IECC students. The student email accounts are cost-effective and environmentally friendly. The IECC email account is IECC's official communication and notification method to students. IECC expects that every student will receive email at his or her IECC email address and will read email on a frequent and consistent basis. A student's failure to receive and read IECC communications in a timely manner does not absolve that student from knowing and complying with the content of such communications.

Copyrighted Material
Users shall not: copy and forward, download, and/or upload to the IECC network or Internet server any copyrighted, trademarked, and other intellectual property without express authorization from the owner of the trademark, copyrights, or intellectual property right.

IECC prohibits the use of peer-to-peer file sharing applications on its network, including wireless network services, to transmit, exchange, or copy any music, software, or other materials which are protected by copyright or intellectual property rights.

Unauthorized copying, use, or distributions of software is illegal, strictly prohibited, and subject to criminal penalties. Penalties for copyright infringement are controlled by the U.S. Copyright Office and can be as high at $150,000 per incident. For additional information, please see the website of the U.S. Copyright Office at www.copyright.gov. Similarly, other intellectual property content owners may take criminal or civil action against a user for unauthorized copying, use or distribution of intellectual property materials. All the content transmitted via e-mail and web publishing must either be the users' own or must be transmitted with express authorization for distribution by IECC or by the individual who owns the trademark, copyright, or intellectual property right.

Inappropriate and Illegal Use of Technology Resources
Examples of inappropriate and illegal use include:

1. Accessing, e-mailing or web publishing of material, including text or images, determined to be obscene and/or pornographic.
2. Use of information technology to facilitate, engage in and/or encourage academic dishonesty.
3. Email distribution or web publishing of derogatory statements intended to offend other individuals, groups, or organizations or which violate IECC's anti-discrimination/harassment policy and procedures. (See policy 100.8 and procedure 100.8 for more information.)
4. Use of information technology resources in a manner that violates this Policy, any other District/College policy, and/or local, state, or federal law.
5. Intentionally infiltrate, or "hack," IECC or other information technology resources.
6. Release viruses, worms, or other programs that damage or otherwise harm IECC or other information technology resources.
7. Knowingly disrupt a system or interfere with another student's, staff or faculty member's or other authorized user's ability to use that system
8. Willfully damage or destroy computer hardware, software, or data belonging to IECC or its users.

Priority Usage of Computer Hardware, Software and/or Facilities
Priority shall be given to classroom activities, assignments and/or research and to IECC faculty, staff, and students.

Lab User Age Restriction
Patrons under the age of 18 who are not enrolled students are not permitted to use the open lab computers without obtaining authorization from college staff.

Student Data Storage
Students are not allowed to store personal work and/or software on the hard drives in the open lab and all students should have a personal storage device or service for saving their work. Any files or software found on the hard drives will be deleted. IECC is not responsible for data lost for any reason including but not limited to: power failure, computer failure, or any other planned or unplanned or unavoidable event or emergency.

Software
IECC may provide access to software and services such as MS Office 365, Google Docs, Adobe, and others. These services are generally provided for free or at a reduced cost to currently enrolled students and/or active employees. IECC must comply with the software license agreements provided by the software vendors and services may be revoked or modified at the vendor's discretion. Students and employees are required to comply with the End User License Agreement (EULA) associate with the

software or service. The software and services may be terminated when students are no longer enrolled or employees are no longer employed.

Network Bandwidth
Network capacity is limited and users must not exceed reasonable usage. IECC has the rights to block, limit, or prioritize traffic for any reason.

Internal Network
Only authorized IECC technical staff are allowed to connect personal computers or other devices to the internal IECC network.

Public Wi-Fi Internet Access
Wireless public Internet access is provided throughout most IECC's campus locations. **Please be advised that the public network does not enforce any security or encryption.** Transmissions of secure information such as ID's, credit card numbers, passwords, etc. may be intercepted by wireless users in or near the open networks. **IECC is not responsible for damage to personal property or other injury, including damage to personal computing devices resulting from software/hardware installation or Internet use.**

Commercial Use
Users shall not use the District's computer network to set up web pages to advertise or sell products or services, solicit sales, or conduct business without prior written approval and, if required, the payment of an appropriate fee.

Sanctions
Alleged violations of this policy will be processed according to the disciplinary policies outlined in the IECC Policies and Procedures Manual, the IECC collective bargaining agreement and the college's catalog. IECC treats access and use violators of information technology resources seriously. IECC computing resources may also be subject to prosecution by state or federal authorities.

IECC has the right to remove, without notice, any material from its system found to be threatening, obscene, and pornographic or which violates the District's anti-discrimination/harassment policy or any other District policy. Such action may result in the termination of the user's account.

Policy Adoption – Administration – Liability
This policy will be reviewed and updated periodically and the current policy, inclusive of any revisions, will be electronically posted on the IECC website.

Implementation

The Chancellor, Presidents, and Chief Information Officer are responsible for supervising adoption of guidelines to implement this policy.

Enforcement

Alleged violations of this policy will be processed according to the disciplinary policies outlined in the IECC Policies and Procedures Manual, IECC collective bargaining agreement and the college's catalog. IECC treats access and use violations of information technology resources seriously. IECC will pursue criminal and civil prosecution of violators as it deems necessary.

Definitions

Account: see Information Technology Account

Administrative Officer: Chancellor, President, Dean or Director to whom an individual reports.
Authorized Users: students, employees, and other constituents of the IECC District.

Data Owner: the author or publisher of the information, data, or software; can be the individual or department that has obtained a license for the District's use of the information, data, or software.

Computing Devices: different classes of computers, servers, and mobile devices. If owned or leased by the District, or if owned by an individual and connected to a District-owned, leased, or operated network, use of these computing devices is covered by the IECC Policy for Responsible Use of Information Technology.

Employee: See Human Resources policy section 400.

Information Technology Resources: equipment or services used to input, store, process, transmit, and output information, including, but not limited to, desktops, laptops, mobile devices, servers, telephones, fax machines, copiers, printers, Internet, email, and social media sites.

Information Technology Account: the combination of a user number, user name, or user ID and a password that allows a student, employee, or other authorized user access to information technology resources.

Network: a group of computing devices that share information electronically, typically connected to each other by either cable, wireless or other technologies.

Software: the programs and other operating information used by a computer.

Student: any person currently participating in any class of instruction offered by or on the premises of the IECC institutions.

Systems: see Information Technology Resources

User: see Authorized User

USER AGREEMENT

I agree to and will abide by the attached policy (200.2) concerning the use of computer, Internet, and web publishing access provided to me through Illinois Eastern Community Colleges (IECC).

I understand that alleged violations of this policy will be processed according to the disciplinary policies outlined in the IECC Policies and Procedures Manual, the IECC collective bargaining agreement and the college's catalog. IECC treats access and use violators of information technology resources seriously. IECC computing resources may also be subject to prosecution by local, state, or federal authorities.

I understand that if I am issued an MFA token and it is misplaced or stolen, I may be charged a $25.00 replacement fee.

I UNDERSTAND THAT I SHOULD HAVE NO EXPECTATION OF PRIVACY OR CONFIDENTIALITY IN THE CONTENT OF ELECTRONIC COMMUNICATIONS OR OTHER COMPUTER FILES SENT AND RECEIVED ON THE DISTRICT COMPUTER NETWORK OR STORED ON ANY IECC INFORMATION TECHNOLOGY RESOURCES. THE DISTRICT INFORMATION TECHNOLOGY DEPARTMENT STARR, COLLEGE TECHNICIANS, OR OTHER DISTRICT EMPLOYEES MAY, AT ANYTIME, REVIEW THE SUBJECT, CONTENT, AND APPROPRIATENESS OF ELECTRONIC COMMUNICATIONS OR OTHER COMPUTER FILES, AND REMOVE THEM IF WARRANTED, REPORTING ANY VIOLATION OF RULES TO THE DISTRICT ADMINISTRATION AND/OR LAW ENFORCEMENT OFFICIALS.

NAME: _____
(signature)

_____
(printed name)

DATE: _____