Acceptable Use Policy for Information Technology and Electronic Resources 4019

Southeastern Illinois College (the "College") provides electronic information resources and other computer-based resources to support the College's educational mission. Students, faculty, staff and others who use the College's computer-based resources are required to adhere to this policy.

This policy applies to all computer hardware and software owned or operated by the College, College electronic mail, College websites, and College on-line services and digital signage systems. "Use" of the College network shall include use of or obtaining access to the wired or wireless network from any electronic device whether or not owned or operated by the College.

Acceptable Use

The use of electronic information resources, other computer-based resources and media (the "System") must be consistent with the mission of the College. You are expected to act responsibly and follow all College policies, procedures and guidelines when using the System. College owned electronic equipment and resources should be restricted to educational and business use. System users have no expectation of privacy in connection with the use of the College's System.

Privileges

Access to the System is a privilege, not a right, and may be denied or revoked at any time. Inappropriate use of the System may result in loss of privileges or other disciplinary actions as the College deems appropriate.

Security of System and Responsibilities of System Users

Security must be a high priority for all users. System users shall not disclose their personal login ID or password/PIN to anyone, including another college employee, or attempt to log into the System as another person.

Users are prohibited from transmitting personal and confidential data including but not limited to personally identifiable information, social security numbers or credit card information through email or other insecure means unless reasonable precautions are taken to encrypt or password protect the information. All System users are required to maintain the confidentiality of student and personnel records.

Email Usage

College provided email accounts are an official means of communication and they are provided for the purpose of facilitating the business and operations of the College. The College often sends email communications to faculty, staff, and students which it expects to be read in a timely manner.

College employees and students should conduct themselves in a professional and appropriate manner in all email communications. Email users are not guaranteed a right of privacy in their email communications. All messages composed, sent, or received on the email system are and remain the property of the College, not the private property of any individual person. The College has the right to inspect, copy, store, and disclose the contents of email messages when the College believes it is necessary to prevent or correct improper use, satisfy a legal obligation, insure proper operation of the email, make necessary repairs or updates to the email system or an individual user's email. In the majority of the above situations, the College will notify the email user before accessing their email account. A clear rationale for email access must be provided to Human Resources and the President prior to any action. Rationale should address safety, security, technical, legal, or other paramount reason. Unauthorized access for casual viewing may lead to disciplinary action including up to termination.

Users are required to act responsibly in regard to the content and maintenance of their electronic mailbox. This includes but is not limited to general maintenance, not engaging in activities that would encourage inappropriate or illegal content, and not engaging in activities compromising System data, integrity, security, or performance. It is the user's responsibility to delete and archive emails so that their mailboxes do not fill up and render the accounts unusable.

Group login accounts for shared mailboxes are not permitted. In cases where multiple users need access to a single mailbox or email address, a shared mailbox, distribution list, or alias can be created with the help of the Office of Information Technology (IT) and approval by your department head and the CIO.

Items deleted from a user's mailbox are temporarily retained on the email server for 14 days. Deleted mailboxes or groups are temporarily retained on the server for 30 days. After such time, these items are permanently deleted from the server.

Personal email accounts may also be used on a limited basis for password resets when other information is provided to identify the individual. For their own personal protection, faculty and staff are discouraged from using their College email account for personal use.

When an individual is no longer a member of the College community, their corresponding email account will be removed, and access will be terminated.

Users of SIC email accounts who are found to be in violation of this Policy may be subject to revocation or limitation of email privileges as well as other disciplinary actions.

Efficient Use of Resources

Users must accept limitations or restrictions on computing resources, such as storage space, time limits or amounts of resources consumed. Users should not engage in any activity detrimentally affecting other users of the System.

User Identification

Concealing or misrepresenting one's identity is a violation of college policies, and is subject to disciplinary action.

Vandalism

Any type of vandalism or attempted vandalism (physical or electronic) to any part of the System, a College computer, computer peripherals**,** the College network, or files of others is prohibited and may result in disciplinary action. Vandalism includes, but is not limited to, malicious destruction or deletion of college information, downloading, uploading, or creation of computer viruses or malware.

Specific Prohibited Uses

In addition to the other prohibitions contained in this policy, the following activities which are unacceptable and may result in disciplinary action, include, but are not limited to:

1. Accessing, retrieving, viewing or disseminating obscene, indecent, sexually explicit or vulgar materials or messages unrelated to the educational mission of the college.

2. Retrieving, viewing or disseminating any material in violation of any federal or state regulation/law or College policy. This includes, but is not limited to, improper use of copyrighted material or intellectual property.

3. Intentionally manipulate information on any sensitive applications such as accounting, student, employee, and business records, or tamper and/or attempt to gain unwarranted access to student or employee personal network files. Sensitive files should be stored in a secure place.

4. Engaging in for-profit commercial activities, including but not limited to, crypto-mining, advertising or sales for personal gain.

5. Sending of SPAM or a chain letter.

6. Soliciting money for religious or political causes unless it is an approved fundraising activity for a student organization.

7. Harassing, threatening, intimidating, or demeaning any person or group of people for any reason, including but not limited to race, color, religion, gender, age, national origin, citizenship status, ancestry, marital status, parental status, pregnancy, family status, military status, sexual orientation, disability, source of income, housing status, or any other category protected by law.

8. Disrupting the educational process or interfere with the rights of others.

9. Disrupting information network traffic or interfere with the network or connected systems.

10. Connecting unauthorized devices on the wired or wireless network, including but not limited to, wireless signal boosters.

11. Circumventing or attempt to circumvent system security measures through the use of software or other measures.

12. Gaining access without permission to the files of others**,** or vandalize another user's data or files.

13. Gaining unauthorized access to College electronic resources or other entities using a College computer and/or network.

14. Improperly forge or alter electronic mail messages, or use an account owned by another user.

15. Invading another person's privacy. This includes, but is not limited to, improperly disclosing personally identifiable information such as name, social security number, address, phone number, or user name and password.

16. Using the System or any system resources to send unsolicited commercial email.

17. Violating any software license agreement.

18. Downloading, copying, printing or otherwise storing or possessing any data, in violation of these rules and/or College policy.

19. Any attempt to hide or conceal activity of a prohibited use.

20. Use of tools designed to perform, including but not limited to, vulnerability and port scanning, penetration testing, packet sniffing, password cracking, encryption circumvention and collection of network information of any kind without the expressed written consent of the College IT Office.

21. Engaging in any unlawful use of the system.

Additional Policy Guidelines for College Employees

Employees are required to maintain a 15+ character password. Employees are required to store passwords in a secure manner.

Employees with any device, including but not limited to cell phones, College owned or personally owned, that access College information without additional authentication/login, are required to protect that information through the use of a password, pin, or biometric technology before that information may be accessed.

Employees are required to store college data and mission critical files on the College network. “Cloud” off-premise storage may only be used to store personal student and employee information where an approved contract or agreement exists between the College and the provider. A copy of the contract or agreement must be on file with both Information Technology and the Business Office. Files stored on a local computer should be temporary and personal or sensitive data limited.

Employees are discouraged from using any portable media or device to store personal or private information. When use is completely unavoidable, reasonable protection of encryption and password protection of that information is required. Any data loss or misuse of personal or private information is a serious matter and the employee(s) involved may be subject to disciplinary or additional action.

Employees are prohibited from setting up any online account on behalf of the college using their personal email. Employees are required to use their College issued email account for SIC related business when setting up any College related online account.

Employees are not allowed to make any modifications to their College issued devices, including but not limited to, swapping or adding an additional hard drive, installing another operating system, any network connectivity changes, or any other change that would prevent the device from receiving software updates, security patches, or management by College IT staff.

Employees may not sell, transfer, or dispose of any College owned equipment that would violate any College policies or procedures, federal or state law, in regards to inventory, data destruction and electronic equipment disposal.

Any activities that would violate this policy for the purpose of College instruction must be submitted in detail and approved each semester in writing to the Office of Instruction and the Office of Information Technology.

Sanctions and Discipline

If an individual engages in any of the prohibited acts listed in this policy, or violates this policy and s/he may be subject to College disciplinary actions including, but not limited to, the following:

1. Suspension or revocation of System privileges;
2. Suspension or termination of employment;
3. Academic suspension or expulsion;
4. Referral to legal authorities for prosecution; and
5. Other sanctions, discipline or action the College deems warranted.

Anyone receiving disciplinary action has the right to an appeal through the College’s Disciplinary Grievance Procedures. Repeated violation of this policy will be grounds for escalated disciplinary action and/or appropriate legal action.

Disclaimer

The College makes no warranties, whether expressed or implied, for the System. The College is not responsible for any damages suffered, including the loss of data, resulting from delays, non-deliveries, deliveries, or service interruptions. Use of information obtained via the System is at the user's own risk. The College assumes no responsibility for the accuracy or quality of information obtained through the System. This policy and all its provisions are subordinate to local, state, and federal statutes.

Questions regarding this Policy should be directed to the below:
Contact the Office of Information Technology (IT)

https://sic.edu/directory/departments/information-technology/

Adopted:
Amended: May 21, 2024/ December 4, 2018/February 17, 2015/January 19, 2012/May 16, 2006
Legal Ref:
Cross Ref: