UCNJ
Union College of
Union County, NJ

Appropriate Use

Purpose

UCNJ Union College of Union County, NJ ("UCNJ") provides access to computer systems and networks it owns or operates to UCNJ students, faculty, administrators, staff, alumni and approved guests in order to promote legitimate educational, research and administrative efforts in keeping with the College's role as an educational institution. Such access has broad impact and imposes certain responsibilities and obligations. Users have the responsibility to use these resources in an efficient, ethical and responsible manner, consistent with the law and the mission of the College. The purpose of this policy is to ensure the appropriate use of the College's information technology ("IT") systems.

Policy

I. General Principles
   a. Appropriate use is always ethical, reflects academic honesty and is exercised fairly with respect to the consumption of shared resources. Users are expected to demonstrate respect for intellectual property, copyright and data ownership, system security mechanisms and individuals' rights to privacy and freedom from intimidation, harassment and annoyance.
   b. This policy governs appropriate use of information technology resources and is based on the following:
      i. UCNJ, as owner or operator of College computer and communications systems, has specific proprietary rights of access, regulation of use, resource allocation and management.
      ii. Authorized users have reasonable expectations of access for legitimate purposes, ownership of intellectual property, including data and ideas, privacy from unauthorized monitoring of electronic files and intrusion and freedom from intimidation, harassment and annoyance.
      iii. Authorized users have the responsibility to utilize UCNJ computer facilities and resources for legitimate College purposes. They must respect the rights of others to privacy and protection of their intellectual property, including data, ideas, and copyrighted material, and freedom from intimidation, harassment and annoyance. As an institution of higher education, UCNJ is committed to providing students and faculty with the opportunity to explore the full potential of electronic communication and data gathering to the extent that this use is ethical, consistent with the mission of the College and does not infringe on others' rights of privacy and access to limited resources. Appropriate use of computer facilities for an educational institution extends beyond specific College-related business, but can be restricted by the College to protect its mission and the rights of other users.

c. The College will make reasonable efforts to ensure that the privacy and security of individual users is protected. However, no user should expect that his/her College electronic mail or personal electronic mail, if accessed using College equipment, is private. Furthermore, the College cannot guarantee that its computer systems and networks are completely secure. By using College computer systems and networks, each user assumes the risks of invasion of privacy and misappropriation of confidential information or material protected by copyright and other intellectual property rights.

II. College Rights of Access

a. As owner or operator of College electronic communications systems, UCNJ has proprietary rights of access, regulation of use and resource allocation and management. The College may exercise these rights when it deems it appropriate and in the best interests of the College. These rights include, but are not limited to, the following authority:

   i. To make and retain copies of College data, including e-mail and any other files deemed appropriate, for a time period determined by the College.

   ii. To access all files maintained on College equipment, including e-mail, for specific authorized purposes, including, but not limited to:

      1. To review files for resource management. This may include analysis of corrupt files, potential threats such as viruses or other malware or files that consume an inordinate amount of resources. This review shall be by file characteristics only, such as origination date, frequency of use or some other resource management criterion, and not file subject matter. In such a case, University I.T. Services will make a reasonable effort to contact the user before any action is taken.

      2. To investigate an allegation of violation of law or College policy or in response to a subpoena. In the case of a subpoena or an allegation of violation of law, authorization for such access must be provided by the Associate General Counsel. In the case of an allegation of violation of College policy, authorization for such access must be provided by the Associate General Counsel in consultation with:

         i. Human Resources if the allegations involve an employee;

         ii. the Vice President of Academic Affairs if the allegations involve a faculty member; or

         iii. the Vice President of Student Development if the allegations involve a student.

      3. To protect legitimate business needs, such as when an employee is unexpectedly absent for an extended time and another employee must assume the absent employee's projects or operational responsibilities. Authorization for such access must be provided by the Associate General Counsel in consultation with Human Resources or the Associate Vice President of Administration, as applicable.

iii. To remove files from College systems, including, but not limited to, the following reasons:

1. To conserve limited resources in accordance with established procedures. These procedures may be based on origination date, frequency of use, file size or other resource management criteria, including the nature of file content. Authorized resource managers will make their best effort to notify file holders of these procedures before removing such files.
2. To purge from College systems illegal files or files that infringe on the rights of other users by inequitably consuming limited resources, abrogating creative property rights or invading privacy (including harassment, intimidation or annoyance).
3. To perform other necessary resource management, after making best efforts to notify the file holder.
4. To limit or otherwise restrict creation or file size of email, Web pages, network storage or other resource allocation to UCNJ faculty, students, staff and alumni or other specifically authorized users of College facilities, as system capacity permits. In doing so, the College seeks not to restrict expression of diverse opinions or viewpoints, but to ensure the efficient management of I.T. resources.

iv. To manage the College's voice, data and video bandwidth to maintain the integrity and robustness of college-owned equipment, data and services, as well as the appropriateness of bandwidth use.

b. These proprietary rights of the College, as applicable, will extend to electronic messages, data or files that are sent or received on a personal, password-protected account on a web-based communication system (such as e-mail, text messaging, and file sharing services) if College equipment is used to access such a personal account, to the extent permitted by law.

c. The College is not liable for loss of data because of systems failures, emergencies or the unauthorized access, use, or corruption of data by any individuals, including College employees.

III. User Responsibilities

a. Authorized users have the responsibility to utilize UCNJ computer facilities ethically, with respect for other users and the limited resources made available to them by the College. These include:

i. Being responsible for all activities performed under their user ID and for all use of resources assigned to them. Sharing IDs and passwords is prohibited.

ii. Being courteous and considerate in using all College computer resources. Users should be sensitive to the needs of others and use only what a reasonable person would consider a fair share of computing, network, and telephone resources.

iii. Respecting the rights of others to privacy, including freedom from intimidation, harassment and annoyance. Users must abide by College guidelines for the distribution of email and may not persist in corresponding with others if they have been notified to cease.

iv. Respecting the intellectual and creative property of others, including data, ideas and copyrighted material. Use of another person's creative property without proper attribution may be considered plagiarism under College policy and constitutes a violation of copyright or other laws.

v. Handling confidential information appropriately. Users should always follow best practices in the transmission and storage of College confidential information. Users must appropriately protect any confidential College information they have on their computers. Users should take particular care to protect confidential data when using public computers, laptop computers, external storage devices (such as external hard drives or flash drives), and home computers, and when emailing or posting confidential data to third party file sharing services.

IV. User Expectations

a. Authorized users of UCNJ computer and network facilities for legitimate purposes have reasonable expectations of:

i. Access to files properly stored under their access privileges and to all UCNJ computer files and facilities that are relevant to the legitimate and appropriate use of such College facilities. Denial of access privileges to College computer files and facilities shall be made only in accordance with this and other College policies and procedures. Access privileges, however, are subject to the availability of such files and the College does not warrant or ensure that files will be preserved and uncorrupted due to human error, equipment failure or the need to purge files for resource allocation purposes. All users are responsible for frequently and appropriately backing up all data to guard against such possibilities.

ii. Respect for the ownership of intellectual and creative property, including data and ideas, in accordance with the United States Copyright Act and relevant state and federal laws.

iii. Limits on the receipt of certain kinds of communications. The College will attempt to strike a balance between the individual user's interest in limiting receipt of certain kinds of communications and the interests of other users in reaching an appropriate audience. However, the College has no control over messages originating from beyond the College community and can exercise only limited control over communications from members of the College community if it is to respect the interests of its members in communicating with each other. To this end, the College will encourage the use of managed organizations (such as those available in the College’s portal or the College’s learning management systems) for general-purpose communications and the use of approved broadcast facilities when they are of potential interest to large numbers of community members. Individual users are expected not to send information except to recipients they reasonably expect to welcome such communications and are expected to honor requests from recipients not to receive further communications.

b. Users should not expect the privacy of personal email or other Web based communications, or of content residing on or transmitted through College equipment. The content of electronic messages and files sent or received through personal accounts on Web-based services such as email, text messaging services, file sharing services, or social media sites often leave copies on the equipment used; if College equipment is used to access such private accounts, the College, to the extent provided by law, reserves the right to access and disclose such content without the consent of the user.

V. Inappropriate Uses

a. Examples of inappropriate uses of UCNJ computer facilities include, but are not limited to:
   - i. Commercial uses not specifically authorized by the College.
   - ii. Copying any College-owned software for any purposes, unless specifically authorized by the copyright and licensing provisions of the software and approved by the College.
   - iii. Any circumvention of UCNJ computer security, including using another user's password, decoding passwords, misrepresentation in order to obtain access to data or computer systems or otherwise devising unauthorized access.
   - iv. Activities that damage or disrupt hardware or communications, such as irresponsible or destructive use of equipment, the use of unauthorized network equipment, including the use of wireless equipment that operates above the 900-Megahertz range, virus creation and propagation, wasting system resources and overloading networks with excessive data.
   - v. Intentional damage to or altering of systems, software, or information owned by others, including individual and College files, except as specifically allowed by the file holder.
   - vi. Using computing resources to access any other computer system (on or off-campus) without authorization.
   - vii. Sending offensive, harassing or threatening messages or repeated sending of unsolicited email after being asked to stop.
   - viii. Illegal use of downloaded copyrighted materials including text, audio, and video. While peer-to-peer (P2P) file-sharing utilities (e.g., BitTorrent) are not illegal and are not banned by the College, it is illegal to download or share copyrighted material that has not been approved for such distribution and such downloading of copyrighted material is a violation of this and other College policies.
   - ix. Disseminating any confidential information unless such dissemination is required by the individual's job at the College and is done securely.

VI. Consequences of Violation of Policy

In the event that the College believes a student or employee has violated any part of this policy, the College may suspend or terminate the employee’s computer and/or network access. In addition, violation of this policy may subject students or employees to disciplinary action, up to and including expulsion from the College or termination from employment.