CONCORD UNIVERSITY
BOARD OF GOVERNORS

Policy No. CU-IT-40 Acceptable Use of Information Technology Policy

Section 1. GENERAL

1.1 Scope: This policy applies to all students, faculty, employees, and anyone else using information technology resources owned and/or operated by the University or any of its entities.

1.2 Effective Date: October 29, 2016.

Section 2. INTRODUCTION

2.1 Information technology is playing an increasingly important role in the fulfillment of our institutional mission and in the lives of the members of the Concord University community. Access to these finite resources is a privilege and is provided with an expectation of responsible and acceptable use. In addition to the principles and guidelines provided in this Acceptable Use Policy (AUP), institutional policies along with certain federal, state and local regulations apply to the use of the information and communication technologies (ICT).

Section 3. GENERAL PRINCIPLES AND GUIDELINES

3.1 The basic premise of this policy is that responsible and acceptable use of the Concord University ICT does not extend to whatever an individual is capable of doing. Instead, certain principles provide a guide to users regarding responsible and acceptable behaviors, and users are responsible for knowing and understanding them. These principles and guidelines include, but are not limited to the following:

3.1.1 The Concord University ICT is a State of West Virginia resource. It is funded and developed for the purpose of promoting and supporting the mission of the University.

3.1.2 Use of the Concord University ICT implies consent to this and all other information technology policies.

3.1.3 Faculty wishing to engage in research that may violate the AUP need to have approval from the Chief Academic Officer (CAO) and the Vice President for Information Technology (VPIT). Requests should be submitted in a timely manner to allow full consideration and to plan for any necessary change management.

3.1.4 Authorized users of the Concord University ICT, or University sponsored resources, are those individuals who have been granted a username and password. The username and password combination is your identity and license to access and use the components of the ICT for which you are specifically authorized.

3.1.5 Authorized users will abide by institutional policies along with applicable local, state and federal regulations.

3.1.6 The resources of the Concord University ICT are finite and shared. Appropriate and responsible use of these resources must be consistent with the common good. The ICT may NOT be used for commercial or profit-making purposes or for the purpose of personal gain. The Office of Advancement, Alumni Association, Mountain Lion Club and the CU Foundation are authorized to use the ICT for fundraising, collecting dues, etc.

3.1.7 The University reserves the right to limit access to the ICT when investigating cases of suspected abuse or when violations have occurred.

3.1.8 The University does not monitor or generally restrict the content of material stored on or transferred through the components of the ICT. However, use of the ICT is a privilege and not intended to serve as a public forum. Therefore the University reserves the right to restrict or deny usage of the ICT when such usage conflicts with the mission of the University.

3.1.9 Users must adhere to the legal and ethical standards governing copyright, software licensing, and intellectual property.

3.2 Violation of these guidelines constitutes unacceptable use of information resources, and may violate other University policies and/or state and federal law. Suspected or known violations should be reported to the Office of Technology Services. The appropriate University authorities and/or law enforcement agencies will process violations. Violations may result in revocation of computing resource privileges; penalties for academic dishonesty; or faculty, staff or student disciplinary action up to and including dismissal, and/or legal action.

3.3 The maintenance, operation, and security of computing resources require responsible University personnel to monitor and access the system. To the extent possible in the electronic environment and in a public setting, a user's privacy will be preserved. Nevertheless, that privacy is subject to the West Virginia Freedom of Information Act, and other applicable state and federal laws, and the needs of the University to meet its administrative, business, and legal obligations.

Section 4. COMMENTARY AND ANALOGIES

4.1 The ICT discussed above consists not only of the superficial wires, equipment and devices of the data, voice, video, and more conventional information networks on our campuses (and the world!), but also the more subtle milieu created by the integration of these technologies into our everyday life situations. In this respect the whole is much greater than the sum of the parts and thus the effect of inappropriate use of these resources can be much greater than might be imagined. This reminder should not necessarily be a cause for hesitation about its use, but serves as a call for thoughtful consideration of action.

4.2 In describing the responsibilities and acceptable behaviors related to the ICT, certain analogies can be drawn. Social norms, behaviors, and responsibilities associated with the use of electronic communication, publication, media, and access authorization are no different than the conventional mediums with which we are all familiar. Examples follow.

4.2.1 Email or electronic mail is just another form of mail.

4.2.2 Posting to a news group is the same as posting a notice or comment on a bulletin board, newsletter, letter to the editor, call to a talk show, etc.

4.2.3 Participating in a chat group is the same as participating in discussions anywhere a group might congregate face-to-face, e.g. in a class, the student center, recreation room, lounge, church group, etc.

4.2.4 Creating a WWW or World Wide Web presence, including Social Media, is comparable to publishing (i.e., making public) your own magazine, memoirs, diary, biography, press release, newsletter etc. Consequently, you are not only, typically, the author but also, perhaps more importantly, you become the editor and publisher and are responsible for your publication from a legal standpoint. Even though Concord University is not the publisher, editor, or author, it is the provider of the resource and, as such, is associated with your publication. Therefore, Concord University maintains the right to restrict or deny use of this resource when usage does not promote or support the mission of the University or the State of West Virginia.

4.2.5 User id and password combinations are your identity and license to use and access limited portions of the IT environment. In this sense they are like your CU identification card or a driver's license. Impersonating another individual, or allowing another to impersonate yourself, is a serious legal violation.

4.2.6 The computing systems used for mail, WWW, and other technologically augmented services are similar to a residence hall room, or assigned work or office space. The space (and some of the content) belongs to Concord University and the State of West Virginia but other personal items in the room belong to you. In this sense CU has an obligation to provide a reasonable amount of security to protect your personal property but cannot assume full responsibility for it nor guarantee full privacy (If you are concerned about the inadvertent disclosure of information you should communicate this information in another way.)

4.3 Similarly, as in your residence hall room or office space, in the course of normal maintenance of the IT environment, certain information may be seen by those attending to the maintenance. All employees of the Office of Technology Services are instructed that the disclosure of this information is a punishable offense (as is willful intrusion without cause). Also, in a similar manner, you are allowed the use of certain space and accoutrements and are expected to utilize them in a responsible manner by taking proper care of these resources, providing reasonable security, and respecting the property and privacy rights of others occupying similar spaces and their assigned and private resources.

Section 5. COMMON FORMS OF VIOLATIONS

5.1 Although most users strive for acceptable and responsible use of the ICT, inexperienced users may unwittingly engage in behaviors that violate the principles and guidelines of responsible and acceptable use. To that end, this section outlines some of the more common forms of violations that occur. These examples should not be interpreted as an exhaustive list of violations. Questions regarding the appropriateness of specific behaviors should be directed to the Office of Technology Services.

5.1.1 Furnishing false or misleading information or identification in order to access another user's account.

5.1.2 Using another person's username/password or letting someone else use your username/password.

5.1.3 Investigating, reading or attempting to access another user's files without permission.

5.1.4 Monitoring the electronic communications of others.

5.1.5 Attempts to access or manipulate certain components of the information technology environment without authorization.

5.1.6 Alteration of software, data, or other files without authorization.

5.1.7 Disruption or destruction of equipment or resources.

5.1.8 Using subterfuge to avoid being charged for computer resources or deliberate, unauthorized use of another user's account to avoid being billed for services.

5.1.9 Copying or attempting to copy data or software without authorization.

5.1.10 Sending email or a program which will replicate itself or do damage to another user's account.

5.1.11 Interfering with legitimate work of another user.

5.1.12 Sending abusive, harassing, or obscene messages.

5.1.13 Viewing or listening to material deemed objectionable according to prevailing community standards, obscene, pornographic, or harassing material in public areas (see ICT Policy on Pornography).

5.1.14 Using peer-to-peer file sharing programs (examples include BitTorrent, Grokster, Kazaa and Limewire). The Director of Networking and Support Services may, at his discretion, grant exceptions permitting the use of peer-to-peer file sharing programs on a case-by-case basis.

5.1.15 On shared computers such as in computer labs, excessive recreational use of resources that prevents academic use by those waiting for an available computer.

5.1.16 Registering a domain name or hostname to any IP address owned by Concord University.

5.1.17 Sending chain letters or unauthorized mass mailings or transmitting a crippling number of files across a network.

5.1.18 Sending hoax messages or forged messages, including messages sent under someone else's username.

5.1.19 Any activity or action that violates the University's Student Code of Conduct or Policies, faculty/staff policies and regulations, or federal, state, or local laws.

Section 6. ENFORCEMENT

6.1 Technology Services is authorized to engage in investigations and apply certain penalties to enforce this policy. These penalties include, but are not limited to, temporary or permanent reduction or elimination of access privileges to any or all of the components of the ICT. If, in the opinion of Technology Services, it is necessary to preserve the integrity of facilities, services, or data, Technology Services may suspend any access, whether or not the account owner is suspected of a violation. In such a case, Technology Services will attempt to notify the user of any such action after the potential threat to the facilities, services, or data is contained. If such an investigation is required, it will be done only under the direct authorization of the VPIT and every effort will be made to avoid disclosure of any content to anyone other than those with a need to know during the investigation or adjudication of the alleged offense.

6.2 Consequences of the discovery and investigation process or even normal maintenance might include the inspection of files contained in an individual's storage space or monitoring selected traffic on the networks. Again, all effort will be made not to disclose any content to anyone other than those with a need to know. However, where there are moral, ethical, or legal implications Technology Services personnel are instructed to contact the VPIT, who may authorize its disclosure to appropriate authorities if deemed warranted, including University, State and Federal law enforcement officials.

6.3 An individual accused of a violation of this policy will be notified and have an opportunity to respond before a final determination of a penalty is made. The VPIT or their designee, in conjunction with other responsible parties (e.g., University Counsel, Student Judicial Affairs, Academic Affairs, or Human Resources) will examine the available evidence and circumstances. If a penalty is levied, the decision may be appealed through the appropriate channels.

6.4 In cases where there is a conflict of interest, or the VPIT is absent, the Chief Human Resources Officer may serve as the VPIT to meet the purpose of sections 6.1, 6.2, and 6.3 above.