Policy Number: 02.046
Policy Title: Use of Communication and Computer Systems
Policy Type: Employee Handbook
Governing Body: Senior Leadership Team
Date of Current Revision or Creation: September 2014

Use of Communication and Computer Systems

Antioch College's communication and computer systems are intended for business purposes and may be used only during working time; however limited personal usage is permitted if it does not hinder performance of job duties or violate any other College policy. This includes the voice mail, e-mail and Internet systems. Users have no legitimate expectation of privacy in any material created, received, or sent from the E-mail system, or in any other information stored on the College's information systems that result from an employee's use of such systems. Antioch College reserves the right to monitor and to access any matter created, received, or sent from the E-mail system or internet, downloaded onto the computers provided by the College or otherwise stored on the College's information systems in regard to their use of the systems.

Antioch College may access the voice mail, e-mail systems and all other electronic information and obtain the communications within the systems, including, without limitation, past voice mail and e-mail messages, without notice to users of the system, in the ordinary course of business when the College deems it appropriate to do so. The reasons for which the College may obtain such access include, but are not limited to: maintaining the system; preventing or investigating allegations of system abuse or misuse; other types of investigations the College deems appropriate; assuring compliance with software copyright laws; complying with legal and regulatory requests for information; and ensuring that College operations continue appropriately during an employee's absence.

Further, Antioch College may review Internet usage to ensure that such use with College property, or communications sent via the Internet with College property, are appropriate. The reasons for which the College may review employees' use of the Internet with College property include, but are not limited to: maintaining the system; preventing or investigating allegations of system abuse or misuse; other types of investigations the College deems appropriate; assuring compliance with software copyright laws; complying with legal and regulatory requests for information; and ensuring that College operations continue appropriately during an employee's absence.

The College may store electronic communications for a period of time after the communication is created. From time to time, copies of communications may be deleted.

The College's policies prohibiting harassment, in their entirety, apply to the use of the College's communication and computer systems. No one may use any communication or computer system in a manner that may be construed by others as harassing or offensive based on race, national origin, sex, sexual orientation, age, disability, religious beliefs or any other characteristic protected by federal, state or local law.

Since the College's communication and computer systems are intended for business use, these systems may not be used to solicit for religious or political causes or outside organizations.

Further, since the College’s communication and computer systems are intended for business use, all employees, upon request, must inform management of any private access codes or passwords.

Computers are typically pre-installed with authorized software, such as operating system, basic word processing, etc., as well as software purchased for authorized purposes.

Unlicensed software may not be installed on any of the College’s computers. Employees must not upload or download any unauthorized software from the Internet, as this poses security and virus infection risks. The College prohibits the installation of freeware and shareware for personal use on its computers. File sharing programs such as Napster, Bear Share, Kazaa, etc. are strictly prohibited and will be removed by the College if found. Such software often opens hidden portals or gateways that breach the security of the College’s network. If shareware is required by a user, it should be registered and documentation of its purchase should be on file with the College. As a rule you may not download freeware or shareware, unless approved by the College.

Additional software beyond what was previously installed or authorized may not be installed on the College’s computers without the express written permission of the College. The College must sign off on the purchase of all software used by employees. If you feel you have a need for software that has not been authorized for you, please discuss your requirements with your department manager.

College-owned software may not be copied for any reason, without the express written permission of the College, and then only for legal internal use. College-owned software may never be distributed to anyone not employed by the College.

User-owned software may not be installed on the College’s computers without the express written permission of the College, and then only if the user can produce proof that the installation would be permitted under the software’s EULA (end user’s license agreement). The license agreement (or other approved documents) that allows use of the software on College equipment must reside in the College’s files as long as the software remains installed on any of the College’s computers.

Employees should not bring personal computers or other equipment such as disk drives or memory sticks to the workplace or connect them to the College’s computers or networks, unless expressly permitted to do so by the College. Any employee bringing a personal computer or other equipment onto the College’s premises thereby gives permission to the College to inspect the computer or other equipment at any time with personnel of the College’s choosing and to analyze any files, other data, or data storage media that may be within or connectable to the computer or other equipment in question.

Employees who become aware of misuse of the E-mail system should promptly contact their manager/Supervisor or the Office of Human Resources.

No employee may access, or attempt to obtain access to, another employee’s computer systems without appropriate authorization.

Violators of this policy may be subject to disciplinary action, up to and including discharge.