

College Manual of Policies and Procedures

Title: Acceptable Use Policy (AUP)	Date: 08/21/2013	Number: 200.101
Section: General Administration/Computer	Maintained by: Technology Advisory Group (TAG)	Created: 12/07/2011 Approved by TAG: 04/24/2013 Last Revised: 08/01/2013 Effective: 02/01/2014 Adopted by BOT: 08/21/2013

I. General Statement of Policy

Cayuga Community College (the “College”) is committed to academic excellence and providing the resources necessary to maintain academic excellence. Pursuant to this goal, computers, computer accounts, network, wireless, Internet access, electronic mail, mobile devices, and related services (individually and collectively, these computing resources and services are referred to as the “computer system”) may be provided for use by members of the College community. This policy applies to any student, faculty member, staff member, employee, or other individual who has received appropriate authorization to use the College’s computer system. Access to and use of the College’s computer system is a privilege, and such use must be consistent with the terms of this policy, and with the goals, standards, and overall mission of the College. Use of the College’s computer system shall constitute the user’s agreement to abide by and to be bound by the provisions of this policy. The College reserves the right to modify this policy at any time in its sole and absolute discretion.

II. Electronic Communications

All messages, data, files, programs, Internet web sites, and other material or information (individually and collectively referred to as “electronic communications”) stored in or transmitted via the College’s computer system are College records. Accordingly, the College reserves the right to access and disclose the content of electronic communications stored in or transmitted via its computer system: (1) as it deems appropriate for the administration and maintenance of the computer system; (2) when the College determines that such access or disclosure is necessary to investigate a possible breach of security, misuse of College resources, violation of law, or infringement of College rules; (3) when the College determines that such access and disclosure is necessary in connection with an academic, disciplinary, or administrative inquiry, or legal proceeding; or (4) for all other purposes permitted by law. The College may routinely monitor and log usage data such as network session connection times and end-points, computer and disk utilization for each user, security audit trails, network loading, etc. Each user’s use of the computer system constitutes consent to the College’s access, disclosure, and monitoring. Users of the computer system should not have any expectation of privacy in any electronic communications stored in or transmitted via the College’s computer system. Intellectual property rights for content of electronic communications are not governed by this Acceptable Use Policy.

III. Acceptable and Prohibited Uses of Cayuga’s Computer System

Acceptable Use

The College’s computer system is provided for the purpose of supporting the educational mission and business functions of the College. All computer system users are expected to use the computer system for legitimate purposes consistent with the educational mission and business functions of the College. The College has sole authority to determine what uses are acceptable and which uses are inconsistent with this policy or other applicable standards of conduct.

The College's computer system shall be used only for official business, except that it may be used for rare and necessary personal purposes, provided that such use is in a limited amount and duration and does not conflict with the proper exercise of the duties of the College employee. Supervisors are authorized to require employees to cease or limit any personal use that interferes with job performance or violates College policy. Incidental, rare personal use of the computer system is a privilege that may be monitored, restricted or revoked at any time.

Prohibited uses of the computer system for all users include, but are not limited to:

- 1) **Engaging in copyright infringement or other unauthorized downloading, copying and/or distribution of copyrighted material**, unauthorized downloading of any copyrighted material (software, MP3s, movies, etc.), (2) copying and/or distributing copies of copyrighted audiovisual works without the authorization of the copyright owner via "peer-to-peer" programs such as KaZaA, LimeWire, BearShare, and Morpheus, and (3) setting up file shares with copyrighted material, violates the U.S. Copyright Act, 17 U.S.C. §§ 101 *et. seq.* and is prohibited by College Policy.

Copyright infringement may subject you to both civil and criminal liabilities: In a civil action, you may be liable for the copyright owner's actual damages plus any profits made from your infringing activity. Alternatively, the copyright owner can elect to recover statutory damages of up to \$30,000 or, where the court determines that the infringement was willful, up to \$150,000. Copyright infringement may also constitute a federal crime if done willfully and: (1) for purposes of commercial advantage or private financial gain; (2) by the reproduction or distribution, during any 180-day period, of 1 or more copies of 1 or more copyrighted works, which have a total retail value of more than \$1,000; or (3) by the distribution of a work being prepared for commercial distribution, by making it available on a computer network accessible to members of the public, if you knew or should have known that the work was intended for commercial distribution (17 U.S.C. § 506). Criminal penalties for infringement may include imprisonment for up to 10 years, fines up to \$250,000, or both (18 U.S.C. § 2319).

Students who violate the College's policy are also subject to discipline under the College's Student Code of Conduct, which may result in sanctions including, but not limited to, written warnings, disciplinary probation, monetary damages and fines, interim suspension, disciplinary suspension and disciplinary expulsion. The sanction imposed for a particular violation will be determined on a case-by-case basis depending on the specific facts and circumstances involved.

- 2) Installing software on the College's computer system without the consent of IT;
- 3) Attempting to access or monitor another user's electronic communications; reading, copying, changing, or deleting another user's messages, files, or software, without permission of the user; or in some other way invading the privacy of others;
- 4) Engaging in any illegal commerce or any illegal activity of any kind;
- 5) Posting or transmitting any material that is threatening, abusive, profane, defamatory, obscene, offensive, or pornographic, or that is discriminatory, harassing, derogatory, or demeaning to any individual or group based on race, color, religion, sex, sexual orientation, gender expression/identity, disability, familial status, age, national origin, ethnicity, or other prohibited basis;

- 6) Engaging in any type of harassment of other individuals, including continually sending unwanted messages after a request to stop;
- 7) Attempting to destroy or sabotage the computer system or attempting to perform any act that impacts upon the proper operation of the computer system, such as intentionally spreading computer viruses;
- 8) "Hacking," tampering, or attempting to gain unauthorized access to confidential information within the College's computer system or to other remote computer systems;
- 9) Releasing confidential or proprietary information or data obtained by virtue of the user's position with the College to unauthorized persons;
- 10) Attempting to subvert security systems or data protection schemes to gain unauthorized access to information or data;
- 11) Performing acts that are wasteful of computing resources or that unfairly monopolize resources to the exclusion of others, such as sending unnecessary mass mailings or chain letters;
- 12) Operating businesses, unauthorized fundraising or using the computer system in some other way for personal gain, for the benefit of a third party, or for activities that are inconsistent with the College's tax-exempt status (such as political campaigning)
- 13) Creating and/or operating web sites on computers on the College network without obtaining prior approval from IT;
- 14) Using the computer system for non-College related uses that result in a negative impact on College-related uses. For example, if you are using a machine in a public computer lab for non-College related purposes, and others are waiting to use a machine for academic purposes, you are expected to give up your seat;
- 15) Extending the network by introducing a hub, switch, router, firewall, wireless access point, server, or any other service or device without obtaining prior approval from IT;
- 16) Using a computer account that does not rightfully belong to you; and
- 17) Giving or publishing a password, identifying code, personal identification number, or other confidential information about a computer, computer system, network or e-mail account, database, or any other College IT resource.

All users of the computer system must act responsibly and maintain the integrity of the computer system. The College reserves the right to limit, restrict, revoke, suspend, deny, or extend computing privileges and access to the computer system. Violators of any computer use policy will be subject to the existing student or employee disciplinary procedures of Cayuga Community College. Illegal acts involving Cayuga Community College computing resources may also subject users to prosecution by local, state, and federal authorities.