ITS Resource Center Home

Policies - Indemnification of Hamilton College

Contact Information

Administrative Services
315-859-4169
its@hamilton.edu

Users agree, in consideration of access to the College's computing, networking and media services, to indemnify, defend, and hold harmless the College for any suits, claims, losses, expenses or damages, including, but not limited to, the user's access to or use of the College's computing, networking, and media services and facilities.

Noncompliance and Sanctions

Information Technology Services may suspend or terminate all computing privileges of any individuals without notice who engage in improper computing activities. Serious cases, as determined by the Vice President for Information Technology, Hamilton College, will be referred to the appropriate officer of the college for disciplinary action. Such disciplinary action may include the suspension, expulsion, or termination of the offending individual, as appropriate and as determined at the sole discretion of Hamilton College. Where violation of state and federal law is involved, cases will be referred to the proper legal authorities for action. The following serves to provide examples of violations of computing or computing facility policies at Hamilton College. The list of violations includes, but is not limited to:

- Malicious misuse. Examples - using IDs or passwords assigned to others, disrupting the network, destroying information, removing software from public computers, spreading viruses, sending e-mail that threatens or harasses other people (a Class A misdemeanor under New York State law), invading the privacy of others, and subscribing others to mailing lists or providing the e-mail addresses of others to bulk mailers without their approval.

- Unacceptable use of software and hardware. Examples - knowingly or carelessly running or installing unlicensed software on any computer system or network; giving another user a program intended to damage the system; running or installing any program that places an excessive load on a computer system or network, or compromises the security of the systems or network; violating terms of applicable software licensing agreements, including copying or reproducing any licensed software; or violating copyright laws and their fair use provisions through inappropriate reproduction or dissemination of copyrighted text, images, or other materials; using imaging equipment to duplicate, alter and subsequently reproduce official documents.

- Inappropriate access. Examples - unauthorized use of a computer account; providing misleading information in order to obtain access to computing facilities; using the campus network to gain unauthorized access to any computer system; connecting unauthorized equipment to the campus network; unauthorized attempts to circumvent data protection schemes to uncover security loopholes (including creating and/or running programs that are designed to identify security loopholes and/or decrypt intentionally secure data); knowingly or carelessly performing an act that will interfere with the normal operation of computers,

terminals, peripherals, or networks; deliberately wasting or overloading computing resources, such as printing too many copies of a document; or other activities.

- Inappropriate use of electronic mail and Internet access. E-mail communications are subject to statements of conduct as published in the Student, Faculty, Administrator, Staff, and Maintenance and Operations Handbooks, as well as all applicable federal and state laws. In addition, other activities that threaten the integrity of the system or harm individual users are not allowed. These include, but are not limited to initiating or propagating electronic chain letters; inappropriate mass mailing including multiple mailings to newsgroups, mailing lists, or individuals, forging the identity of a user or machine in an electronic communication or sending anonymous e-mail; using another person's e-mail account or identity to send e-mail messages; attempting to monitor or tamper with another user's electronic communications; reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner; or using e-mail or personal web page advertising to solicit or proselytize others for commercial ventures, religious or political causes, or for personal gain.

Last Updated: January 10, 2012