ACCEPTABLE USE OF NETWORKING AND COMPUTER RESOURCES AT THE ART INSTITUTE OF CHICAGO AND THE SCHOOL OF THE ART INSTITUTE

Policy number: 051
Policy applies to: All AIC and SAIC employees
Last updated date: February 22, 2016

I Purpose

The purpose of this policy is to support the Institute's mission and goals and to abide by internal policies as well as local, state and federal law.

II Procedure

The Art Institute of Chicago (AIC), encompassing both the museum and the School, provides access to local, national and international networks as well as computing resources in order to support its mission and goals.

General Principles

Access to network and computing resources owned or operated by the AIC imposes certain responsibilities and obligations and is granted subject to all AIC policies as well as local, state and federal laws. Acceptable use should always be legal and ethical, reflect academic honesty, show restraint in the consumption of shared resources, and reflect community standards. It should demonstrate respect for intellectual property, ownership of data, system security mechanisms, and individuals' rights to privacy and freedom from intimidation and harassment based on race, gender, sexual orientation, disability, national origin or any other status protected by law.

Guidelines

There are responsibilities that must be met as a part of the privilege to access network and computing resources. These include, but are not limited to, the following:

You must not:

1. Use resources to engage in unlawful activities, including sending discriminatory or harassing remarks or content or threats of violence.
2. Allow other individuals to use or fail to protect your assigned accounts (user ids), passwords and access assigned to you.

3. Access or attempt to access another user's accounts, passwords, computers, data, files, or e-mail without authorization.
4. Misrepresent yourself or attempt to circumvent any data protection or network security measures.
5. Use network resources to gain or attempt to gain unauthorized access to remote computers.
6. Attach any equipment, including wireless access points, or install any software that could potentially impair the performance, integrity or security of any AIC computers, networks or data.
7. Attempt to decode passwords or data or to monitor another user's communications.
8. Deliberately perform an act that interferes with the operation of computers and/or network traffic.
9. Engage in any activity that could be purposely harmful to systems or information such as creating or propagating viruses, disrupting services, damaging files, or making unauthorized modifications to data.
10. Use resources for commercial profit making purposes without authorization.
11. Use resources for political purposes that are incompatible with AIC's non-profit status.
12. Perform acts that unfairly monopolize resources to the exclusion of other authorized users.
13. Violate the terms of any software licensing agreements and copyright laws.
14. Infringe any copyright, including the unauthorized and infringing distribution of copyrighted materials through unauthorized peer-to-peer file sharing.
15. Engage in any other activity that does not comply with the General Principles presented above.

Enforcement

The AIC considers any violation of acceptable use principles or guidelines to be a serious offense. The AIC reserves the right to copy and/or examine any files or information resident on AIC resources allegedly related to unacceptable use. In cases of misuse or abuse which involve an immediate threat to the network, data or rights of other users, the AIC has the right to temporarily suspend a user's access or to disconnect the offending system or network subdivision to which it is attached without prior notice. Violators are subject to disciplinary actions as outlined in the student, faculty and staff handbooks or in AIC/SAIC policy statements. Access to network and computing resources owned or operated by the AIC will be terminated, in appropriate circumstances, for individuals who are repeat infringers of third party copyrights.

Users should also be aware that copyright infringement, including the unauthorized and infringing distribution of copyrighted materials through unauthorized peer-to-peer file sharing, may result in civil and criminal liabilities under federal copyright law.

Civil liabilities may include actual damages and the infringer's profits, or statutory damages for each work infringed ranging from $750 to $30,000 (or up to $150,000 in the case where the infringement was committed "willfully"). (17 U.S.C. 504) An infringer may also be subject to criminal liability for willfully infringing a copyright (A) for purposes of commercial advantage or

private financial gain; (B) by the reproduction or distribution, including by electronic means, during any 180-day period, of one or more copies or phonorecords of one or more copyrighted works, which have a total retail value of more than $1,000; or (C) 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 such person knew or should have known that the work was intended for commercial distribution. (17 U.S.C. 506)

Information Disclaimer

Individuals using network and computing resources at AIC do so subject to local, state and federal laws and all policies in effect at the museum and the School. Information, messages and materials made available via AIC network resources do not necessarily reflect the attitudes, opinions or values of the Art Institute of Chicago, its faculty, staff, or students.

Title of policy owner: Chief Information Officer
Department: Information Services
Approval: Chief Information Officer
Revision date history: February 22, 2016
Originally issued date: July 1, 2009
Refer questions to: policyquestions@artic.edu