NETWORK ACCEPTABLE USE

Policy 271

Purpose

The College Network incorporates all electronic communication systems and equipment at Glen Oaks Community College (the "College"). This Network Acceptable Use Policy ("AUP") sets forth the standards by which all Users may use the shared College Network. The College Network is provided to support the College and its mission of education, service, and research. Any other uses (other than permitted personal use as discussed below), including uses that jeopardize the integrity of the College Network, the privacy or safety of other Users, or that are otherwise illegal are prohibited. The use of the College Network is a revocable privilege.

By using or accessing the College Network, Users agree to comply with this AUP and other applicable College policies which may be implemented from time to time, as well as all federal, state, and local laws and regulations. Only Users are authorized to use and/or access the College Network. The term "User" refers to any faculty, staff, or student associated with the College, as well as any other individual with access to computers or other network devices that have been approved by the Director of IT or Vice-President of Finance and Administrative Services for connection to the College Network. This definition includes, but is not limited to, contractors, visitors, and temporary affiliates.

Principles

General requirements for acceptable use of the College Network are based on the following principles:

A. Each User is expected to behave responsibly with respect to the College Network and other Users at all times.

B. Each User is expected to respect the integrity and the security of the College Network.

C. Each User is expected to behave in a manner consistent with the College's mission and comply with all applicable laws, regulations, and College policies.

D. Each User is expected to be considerate of the needs of other Users by making every reasonable effort not to impede the ability of others to use the College Network and show restraint in the consumption of shared resources.

E. Each User is expected to respect the rights and property of others, including privacy, confidentiality and intellectual property.

F. Each User is expected to cooperate with the College to investigate potential unauthorized and/or illegal use of the College Network.

G. Each User is expected to respect the security and integrity of College computer systems and data.

H. Users will properly log out of sessions.

I. Users will monitor access to their accounts. If a user suspects unauthorized activity or that their account has been compromised, they must report the compromise to the Director of IT, and change passwords immediately.

J. Users will use only supported and patched applications and operating systems on college-owned devices. Exceptions must be documents and approved by the Director of IT.

Prohibitions

Without limiting the general guidelines listed above, unless expressly agreed to by the Director of IT, the following activities are specifically prohibited:

A. Users may not attempt to disguise their identity, the identity of their account or the machine that they are using. Users may not attempt to impersonate another person or organization. Users may likewise not misuse or appropriate the College's name, network names, or network address spaces.

B. Users may not attempt to intercept, monitor, forge, alter or destroy another User's communications. Users may not infringe upon the privacy of others' computer or data. Users may not read, copy, change, or delete another User's data or communications without the prior express permission of such other User.

C. Users may not use the College Network in a way that (a) disrupts, adversely impacts the security of, or interferes with the legitimate use of any computer, the College Network or any network that the College connects to, (b) interferes with the supervisory or accounting functions of any system owned or managed by the College, or (c) take action that is likely to have such effects. Such conduct includes, but is not limited to: hacking or spamming, placing of unlawful information on any computer system, transmitting data or programs likely to result in the loss of an individual's work or result in system downtime, sending "chain letters" or "broadcast" messages to lists or individuals, or any other use that causes congestion of any networks or interferes with the work of others.

D. Users may not distribute or send unlawful communications of any kind, including but not limited to cyber stalking, threats of violence, obscenity, child pornography, or other illegal communications (as defined by law). This provision applies to any electronic communication distributed or sent within the College Network or to other networks while using the College Network.

E. Intentional access to or dissemination of pornography by College employees, temporary staff, contractors, or vendors is prohibited unless (1) such use is specific to work-related functions and has been approved the respective manager or (2) such use is specifically related to an academic discipline or grant/research project. This provision applies to any electronic communication distributed or sent within the College Network or to other networks while using the College Network.

F. Users may not attempt to bypass network security mechanisms, including those present on the College Network, without the prior express permission of the owner of that system. The unauthorized network scanning (e.g., vulnerabilities, post mapping, etc.) of the College Network is also prohibited. For permission to perform network scans, user must receive prior approval by calling the Director of IT.

G. Users may not engage in the unauthorized copying, distributing, altering or translating of copyrighted materials, software, music or other media without the express permission of the copyright holder or as otherwise allowed by law. Information on the Digital Millennium Copyright Act can be found at:

http://www.copyright.gov/legislation/dmca.pdf and the Copyright Act at: http://www.copyright.gov/title17/

H. Except as allowed under the Personal Use Policy or the Policy on Use of College Resources in Support of Entrepreneurial Activities. Users may not use the College Network for private business, commercial or political activities, fundraising, or advertising on behalf of non-College organizations, unlawful activities, or uses that violate other College policies.

I. Users may not extend or share with public or other users the College Network beyond what has been configured accordingly by Director of IT. Users are not permitted to connect any network devices or systems (e.g., switches, routers, wireless access points, VPNs, and firewalls) to the College Network without advance notice to and consultation with the Director of IT. To contact the Director of IT, users must call Extension 315 and submit an IT request form.

J. Users are responsible for maintaining minimal security controls on their personal computer equipment that connects to the College Network, including but not limited to: current antivirus software, current system patches, and strong passwords.

K. Users may not violate any laws or ordinances, including, but not limited to, laws related to copyright, discrimination, harassment, threats of violence and/or export controls.

L. Users will not share access codes, PINS, MFA Tokens, or passwords.

M. Users will use MFA when possible on all systems containing sensitive or restricted data.

Review and Penalties

The College reserves the right to review and/or monitor any transmissions sent or received through the College Network. Access to other transmissions sent or received through the College Network may occur in the following circumstances:

A. In accordance with generally accepted, network-administration practices;

B. To prevent or investigate any actual or potential information security incidents and system misuse, if deemed necessary by authorized personnel;

C. To investigate reports of violation of College policy or local, state, or federal law;

D. To comply with legal requests for information (such as subpoenas and public records requests); and

E. To retrieve information in emergency circumstances where there is a threat to health, safety, or College property involved

Penalties for violating this AUP may include:

A. Restricted access or loss of access to the College Network;

B. Disciplinary actions against personnel and students associated with the College,

C. Termination and/or expulsion from the College, and

D. Civil and/or criminal liability.

The College, in consultation with its legal counsel, may contact local or federal law enforcement authorities to investigate any matter at its sole discretion.

Policy Updates

The College reserves the right to update or revise this AUP or implement additional policies in the future. Users are responsible for staying informed about College policies regarding the use of computer and network resources and complying with all applicable policies. The College shall provide notice of any such modifications or amendments by email to the College community. Any such modification shall be effective immediately upon notice being provided regardless of whether subscriber actually reads such notice.

Policy History: Adopted by Board of Trustees 4/9/97, revised 6/9/99, 1/12/20, 10/13/04 6/11/14, 12/8/22, 4/13/2023