POLICY STATEMENT ON THE USE OF COMPUTER AND INFORMATION RESOURCES

Quinnipiac University provides an extensive array of computer and information technology to students. Users are provided access to internet and networking resources including software applications and library databases.

Students are encouraged to explore and utilize computer and information resources within the limits of their Quinnipiac account, share their computer knowledge and expertise with other Quinnipiac users, facilitate the legitimate access to computer and information resources by other Quinnipiac users, and create and freely distribute original software and documentation designed to enable other Quinnipiac members to use the resources more effectively. Our campus community depends heavily on Quinnipiac's network to complete essential parts of their academics and daily work; therefore, users must not intentionally damage or misuse system resources so as to prevent others from doing their work or completing their studies.

The provision of computing resources at Quinnipiac requires strictly legal and ethical utilization by all users including faculty, students and staff. The computing facilities at Quinnipiac, including all network resources, all school and departmental computers and labs along with network and internet bandwidth resources are limited and should be used in a responsible manner.

Inappropriate use of resources includes such activities as:

- Using computer and network resources for personal nonacademic activities, which denies computer and network access for academic purposes
- Using Quinnipiac's network resources to illegally share or distribute copyrighted material (including movies, music and software)
- Unauthorized distribution of copyrighted material, including peer-to-peer file sharing, may subject a student to civil and criminal liabilities

Summary of Civil and Criminal Penalties for Violation of Federal Copyright Laws

Copyright infringement is the act of exercising, without permission or legal authority, one or more of the exclusive rights granted to the copyright owner under section 106 of the Copyright Act (Title 17 of the United States Code). These rights include the right to reproduce or distribute a copyrighted work. In the file-sharing context, downloading or uploading substantial parts of a copyrighted work without authority constitutes an infringement.

Penalties for copyright infringement include civil and criminal penalties. In general, anyone found liable for civil copyright infringement may be ordered to pay either actual damages or "statutory" damages affixed at not less than $750 and not more than $30,000 per work infringed. For "willful" infringement, a court may award up to $150,000 per work infringed. A court can, in its discretion, also assess costs and attorneys' fees. For details, see Title 17, United States Code, Sections 504, 505.

Willful copyright infringement can also result in criminal penalties, including imprisonment of up to five years and fines of up to $250,000 per offense. For more information, go to copyright.gov (https://copyright.gov) to view the website of the U.S. Copyright Office. Also visit copyright.gov/help/faq (https://copyright.gov/help/faq/) to view the FAQ section.

- Sending harassing, pornographic, inappropriate or frivolous messages (including email, social media posts and SMS text via mobile devices), either locally or over the internet
- Using excessive amounts of storage on Office 365, MyFileSpace or MyWebSpace
- Using excessive bandwidth
- Running grossly inefficient programs

These guidelines, though not covering every situation, specify some of the responsibilities that accompany computer usage at Quinnipiac and the networks to which Quinnipiac is connected. All users are expected to abide by these regulations and by the regulations governing the use of the campus computers, computer networks and labs.

Responsibilities of Each Computer User's Use of Computer Resources

Every member of the Quinnipiac community must use computer and network resources only for the purpose for which they are intended. No one has the right or authority to extend their established range of access to computer systems or records. Quinnipiac-supported computing includes unsponsored research, instructional computing, learning and administrative activities. Resources must not be used for commercial purposes or personal monetary gain.

System Security and Privacy

The security of institutional records is the responsibility of each member of the faculty, staff and student body. Institutional records include all matters pertaining to personnel, payroll, registrar, admissions, financial aid, development, medical records, security reports, financial data and other information of privileged and private nature.

Users must not attempt to modify system access, attempt to disrupt the system or attempt to subvert the restrictions associated with their computer accounts. They should not tamper with any software protection placed on any computer applications (e.g., antivirus software).

Users must not search for, or use software to scan the network for, access or copy directories, programs, files, disks or data belonging to others without specific authorization to do so. Programs and data residing in Quinnipiac University departmental systems are not considered public domain and should not be used, in part or in whole, for any purpose other than that which is officially authorized.

Quinnipiac-provided computing equipment and software must not be used to violate the terms of license agreements, and all users must comply with federal and state laws, and all university regulations, related to copying, distribution and use of computer software and data.

Any violation of this policy will be considered a serious matter and be dealt with accordingly.

Choosing Passwords

Passwords are an essential aspect of computer security, providing important front-line protection for electronic resources by preventing unauthorized access. Passwords help the university limit unauthorized or

inappropriate access to various resources including user accounts, web and email accounts.

Users must choose difficult-to-guess passwords. Passwords must not be found in the dictionary and must not be a reflection of the user's personal life. All passwords must be at least eight characters. Users must choose passwords that include both alphabetic and numeric characters, upper and lower case and special characters ($, %, @, $, etc.). An example would be @Qu2018! Or N0t2hrd?.

Changing Passwords

User-chosen passwords must not be reused or recycled. Passwords must be changed at least once a year and passwords must be changed the first time they are used. If a user suspects that somebody else may know their password, the password must be changed immediately.

User passwords can be reset at go.qu.edu/myqpassword (https://account.activedirectory.windowsazure.com/securityinfo/#/register) or by contacting the Information Services Help Desk.

Protecting Passwords

Users must not share a password with anyone, including other users, parents, students, staff and faculty. Users must not store passwords in any computer files, such as logon scripts or computer programs, unless the passwords have been encrypted with authorized encryption software. Passwords must not be written down unless they are physically secured, such as placed in a locked area (e.g., locker or safe).

Individual Security and Privacy

A user must use only their own computer account. The structure of accounts and passwords plays an important role in protecting the work and privacy of all users. You must log in only to your own account (except for extraordinary situations where staff receives a user's permission to access the account temporarily for troubleshooting purposes).

Out of respect for personal privacy, Quinnipiac does not examine the contents of files in user accounts except in response to user requests for assistance, or in circumstances when system security, physical security/safety or troubleshooting procedures require it. Whenever the contents of a user's file must be examined, an effort first will be made to notify the user and invite them to be present. However, if the system is under immediate threat, appropriate actions may be taken without prior notice to the user.

A user is responsible for all use made of their account, and may not authorize anyone else to use their account (except as mentioned above).

The user must take all reasonable precautions, including password maintenance and file-protection measures, to prevent its unauthorized use. While Quinnipiac University provides anti-virus software, it cannot protect against users downloading and installing malicious software.

All users are responsible for keeping their computers free of malicious software that presents a danger to themselves, other systems and network resources.

Installation of devices on Quinnipiac's network infrastructure that causes disruption to operations, either deliberate or accidental, is prohibited. Students need to check with the Help Desk before adding devices such as (but not limited to) wireless access points, switches, routers, DHCP servers, or radio devices operating in the ISM band (802.11 A,B, G,N and AC).

Consequences

Abuse of computing privileges may be subject to disciplinary action, as established by the operating policies and procedures of Quinnipiac, and may result in the loss of computer privileges. Abuse of the network or of computers at other sites connected to the network will be treated as abuse of computing privileges at Quinnipiac. It should be understood that this policy does not preclude enforcement under the laws and regulations of the state of Connecticut and/or the United States of America.