QUEENS UNIVERSITY OF CHARLOTTE

Queens University of Charlotte Acceptable Use Policy For Information Technology Systems

1.0 Overview

The Queens University of Charlotte network is provided as a service to students, faculty, staff, and other members of the Queens community. Maintained by the university's Information Technology Services Department (ITS), the Network supports the educational and service mission of the University.

It is the responsibility of everyone (employees and students) who uses the Queens Network to know these guidelines and to act appropriately and responsibly when utilizing these resources.

Furthermore, users must keep in mind that networks or systems outside of this University (including those in other countries) may have their own distinctive policies and procedures. Users are advised to learn and abide by the policies and procedures of these external networks.

2.0 Purpose

2.1 Overview

The purpose of this policy is to outline the acceptable use of computer equipment and technology resources at Queens University of Charlotte. These rules are in place to conserve finite technology resources for all users and to protect the faculty, staff and students as well as the institution. Individuals are also subject to federal, state and local laws governing many interactions that occur on the Internet. Inappropriate use may expose Queens or individual users to risks including virus attacks, compromise of network systems and services, and legal issues. The University's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to Queens' established culture of openness, trust and integrity.

2.2 Academic Freedom

Queens University of Charlotte's Acceptable Use Policy for Information Technology Systems affirms the principle of academic freedom in the pursuit of scholarship and teaching.

3.0 Scope

This policy applies to faculty, staff, students, contracted employees, temporaries, and other workers at Queens including all personnel affiliated with third parties. This policy applies to all technology systems that are owned or leased by the University. Technology-related systems, including but not limited to, university bandwidth, network infrastructure, any telephone line owned or leased by Queens, software, public computer labs, operating systems, storage media, network accounts providing electronic mail and Web services are the property of the University.

4.0 Policy

4.1 Privacy and Monitoring

1. Queens desires to provide a reasonable level of privacy for its users. However, because of the need to protect the Queens network, ITS cannot guarantee 100% confidentiality of information stored on any network device belonging to the University.
2. For security and network maintenance purposes, authorized individuals within ITS may monitor equipment, systems and network traffic at any time.
3. In addition to the authorized actions of system administrators, e-mail can end up in the hands of ITS staff if it was inaccurately addressed and could not be delivered. Addressing mistakes may also result in private messages appearing in the mailboxes of those other than the intended recipient.
4. Queens reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts.

2. Because information contained on portable computers is especially vulnerable, special care should be exercised.
3. All hosts that are connected to the Queens network, whether owned by an employee or student shall be continually executing approved virus-scanning software with a current virus database.
4. All users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Certain employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).
Under no circumstances is an employee or student of Queens authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing Queens-owned resources.

System and Network Activities

The following activities are strictly prohibited:

1. Accessing an account for which you are not an authorized user.
2. Circumventing user authentication or security of any host, network or account.
3. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
4. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee or student is not an intended recipient or logging into a server or account that the employee or student is not expressly authorized to access. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
5. Port scanning or security scanning is expressly prohibited unless prior notification to the Queens IT Services Department is made.
6. Executing any form of network monitoring which will intercept data not intended for the employee's or student's host computer, unless this activity is approved by ITS.
7. Interfering with or denying service to another authorized user (for example, by changing another user's password without their knowledge or consent or by conducting a denial of service attack).
8. Unauthorized connecting of equipment to the campus network. Students may connect personal computers and laptops to the campus network within their dorm rooms or publicly provided data ports such as those in the Library. Network printers, hubs, switches, wireless devices and servers of any kind may not be connected without approval of the IT Services Department.
9. Use of static IP addresses without first being approved and assigned by ITS.
10. Using a University computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment, hostile workplace, or child pornography laws or is otherwise damaging to the institution. Users are reminded that sexually suggestive materials displayed inappropriately in public places such as the classroom, computer labs or the workplace may constitute sexual harassment.
11. Using University resources for non-academic commercial activity such as creating products or services for sale without express University approval.
12. Providing information about, or lists of, Queens University of Charlotte employees or students to parties outside Queens.

Licensing and Copyright Policies

The following activities are strictly prohibited:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed. The software provided through the University for use by faculty, staff, and students may be used only on computing equipment as specified in the various software licenses.
2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which Queens University of Charlotte or the end user does not have an active license is strictly prohibited. This includes the unauthorized downloading, duplicating or transmitting of copyrighted music files (e.g. MP3 or WMA files etc.) via file sharing software such as Morpheus, KaZaA or similar programs in violation of federal law.

Email and Communications Activities

The following activities are strictly prohibited:

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

It is understood that users may unwittingly create problems for others by, for example, employing programs that monopolize the network bandwidth. In such cases a member of the Queens Staff or Administration will contact the user and explain why and how the user needs to modify his or her electronic behavior.

Access to computing resources may be suspended temporarily at any time if there is clear evidence to suggest that the resource(s) are being used in a manner that seriously compromises the security and/or integrity of the resource(s).

Any employee or student found to have violated this policy may be subject to disciplinary action.

6.0 Definitions

Term	**Definition**
Queens	Queens University of Charlotte
The University	Queens University of Charlotte
ITS	Queens Information Technology Services Department
Spam	Unauthorized and/or unsolicited electronic mass mailings.