PAUL QUINN

Paul Quinn College Information Systems Policies

STATEMENT

Paul Quinn College (PQC) supports the responsible use of its information systems. PQC's information systems include, but are not limited to, computers, servers, wired and wireless networks, computer-attached devices, network-attached devices, voice systems, and computer applications. The use of information resources is for PQC academic activities, research and public service. Access to PQC's information systems is a privilege. All users of information systems should act responsibly to maintain the integrity of these resources. Furthermore, all users shall abide by existing PQC codes of conduct as well as local, state, and federal statutes. PQC reserves the right to limit, restrict, or extend privileges and access of its system to users at any time and for any reason under the college's mission. Any questions regarding PQC Information Systems should be submitted to the Information Technology Director.

NETWORK POLICIES

The purpose of the Information Technology policy is to ensure an information infrastructure that promotes the basic mission of PQC emphasizing academic excellence, high achievement, intellectual and personal integrity and participation in community life. Information resources are powerful, yet necessary, tools for accessing and distributing information and knowledge. Authorized information resource users must be aware of the rights of others to their privacy, intellectual property and other rights. This policy codifies what is considered appropriate use of PQC's information technology.

This policy applies to PQC students, faculty, staff, and to others granted use of PQC information technology and governs the use of information systems whether individually controlled or shared, stand-alone or networked. It applies to all electronic information, audio-visual and communication resources owned, leased, operated or contracted by PQC, including the network, personal computers, workstations, servers, associated peripherals, audio-visual equipment and software.

PQC does not exist in isolation from other communities and jurisdictions and their laws. As a result of investigations, subpoena or lawsuits, PQC may be required by law to provide records or other information related to those records or related to the use of information resources.
Users of information and audio-visual resources must not access computers, audio-visual equipment, software, data or information or networks without proper authorization, or intentionally enable others to do so.

RESPONSIBILITIES

- It is the responsibility of all individuals using PQC's information systems to protect the privacy of their account(s). Personal account information should not be released to friends,

relatives, roommates, etc. Users are responsible for the security of their passwords. Passwords should be changed on a regular basis.

- All individuals using PQC information systems are prohibited from using a computer account for which they are not authorized, or obtaining a password for a computer account not assigned to them.

- The owner or designated assignee of a computer that is attached to the PQC network is responsible for both the security of the computer system and for any intentional or unintentional activities from or to the network connections. Owners or designated assignees are responsible for all network activity originating from their equipment, regardless of who generates it.

- Any person operating a network-intensive application or a defective computer that causes network overload shall be notified, and steps shall be taken to protect other users and the overall PQC network. This may include disconnecting the defective computer system from the network until the problem is resolved. If the condition is an imminent hazard to the PQC network or disrupts the activities of others, the defective computer system or the subnet to which it is attached may be disabled without notice. The operator of the defective computer system shall be expected to follow instructions from networking staff for securing the machine.

- Any person using e-mail should not send excessive e-mail (electronic chain letters), attachments, or messages locally or over the network.

- All copyrighted software, material, or internet content musts not be copied or illegally viewed except as specifically stipulated by the copyright owner or otherwise permitted by copyright law. Copied material must be properly attributed. Computer and communication information this is plagiarized or illegally obtained is subject to the same sanctions as to any other medium. PQC reserves the right to restrict or block TCP or UDP ports of maintain operational efficiency, especially in cases of suspected copyright violations as part of the network policies stated above.

- The content of any files or services made available to others over the network is the sole responsibility of the person with ownership of and/or administrative authority over the computer providing the service. It is this person's responsibility to be aware of all applicable federal and state laws, as well as PQC policies. This person shall be liable for any violations of these laws and policies.

- It is the responsibility of every person using PQC's information resources to refrain from engaging in any act that may seriously compromise, damage, or disrupt the operation of computers, terminals, peripherals, or networks. This includes, but is not limited to, tampering with components of a local area network (LAN) or the backbone, blocking communication lines, interfering with the operational readiness of a computer,

creating/operating unsanctioned servers or personal Web (NAT, DHCP or BOOTP servers included) or File Transfer Protocol (FTP) sites, or delivering unsanctioned streaming audio, video, high bandwidth gaming, or high bandwidth video conferencing. Users should refrain from using an IP address not specifically assigned to them and should not attempt to create unauthorized network connections or unauthorized extensions, or re-transmitting any computer or network services.

- All breaches of system security shall be reported immediately to Administration.

INFRACTIONS

Examples of infractions include, but are not limited to:

- Circumventing or attempting to circumvent data protection schemes or exploiting security loopholes.

- Running programs that attempt to identify passwords, weaknesses in the PQC system, or other security codes.

- Attempting to monitor or tamper with another user's data communications or network traffic, or reading, copying, changing, or deleting another user's files or software without the explicit agreement of the owner.

- Knowingly running or installing on any computer system or network, or giving to another user, a program intended to damage or to place an excessive load on a computer system or network. This includes, but is not limited to, programs known as computer viruses, Trojan horses and worms.

- Using PQC computer resources for private business or commercial activities (except where such activities are otherwise permitted or authorized), fundraising or advertising on behalf of non-PQC organizations, reselling of PQC computer resources, and using PQC's name in an unauthorized manner.

- Engaging in unlawful communications, including threats of violence, obscenity, child pornography and harassing communications.

- Attempting to alter any PQC computing or networking components (including, but not limited to, switches, routers and data/phone/cable TV wiring) without authorization or beyond one's level of authorization.

- Failing to comply with requests from appropriate PQC officials to discontinue activities that threaten the operation or integrity of computers, systems, networks, or otherwise violate this policy.

PENALTIES
Misuse of computing, networking or information resources may result in the loss of computing privileges, as well as other disciplinary action. Furthermore, some misuse may be seen as criminal in nature by either PQC, local law enforcement, or national agencies. Should a user's activity become criminal in nature, PQC reserves the right to provide law enforcement a user's network activity logs.

PRIORITIES
When demand for computing resources exceeds available capacity, priorities for their use shall be enforced. The priorities for use of computing resources are:

- Highest: Uses that directly support the educational, research and service missions of PQC.
- Medium: Uses that indirectly benefit the education, research and service missions of PQC, as well as reasonable and limited personal communications.
- Lowest: Recreational use, including game playing and general browsing.
- Forbidden: Uses listed in the Infractions section of this policy, as well as breaches of the Responsibilities section not specifically listed under the Infractions section.

PQC may enforce these priorities by restricting or limiting usages in circumstances where their demand and limitations of capacity impact or threaten to impact usages of higher priority.

ELECTRONIC USER ACCOUNTS
PQC student electronic user accounts, specifically the Microsoft Outlook Email, CAMS Student Portal and CANVAS Learner Management Platform, assigned to students shall be considered the official method of communication from college faculty, staff and administrators to faculty, enrolled students and staff members, either collectively or individually.

PQC electronic usernames, passwords, access and their contents are owned by the College. If necessary, the College will access former or current student electronic user accounts to determine the source or extent of data security breaches. It is the responsibility of each enrolled student to check for and appropriately respond to all email messages on a regular and frequent basis. Additionally, it is the responsibility of each student to report abnormalities with their electronic user accounts to the Department of Information Technology, using the Helpdesk Process. Students are responsible for protecting username and passwords assigned to them for the use of the campus email system, the CAMS Student Portal and the CANVAS system. Students are advised NOT to open attachments or click on links from unknown sources. Additionally, Paul Quinn College will not ask a student to provide personally identifiable information via email, such as birthdate or social security number. Students are advised to update their passwords on a regular basis.

College officials will use the College's communication system to communicate official messages about advising and degree plans, event dates, new policies, important dates, career fairs and job announcements, residence hall announcements, town hall meetings and other messages deemed important to student life.

Paul Quinn College is firmly committed to data security. To restrict unauthorized access and to ensure data integrity and security, Paul Quinn College implements physical, electronic and administrative policies and procedures intended to safeguard information the College collects

and/or stores. However, the College cannot assure or warrant absolute data security.

IMPLIED CONSENT & LIABILITY RELEASE

All individuals with access to PQC computing resources are responsible for their appropriate use. Such use constitutes an agreement to comply with applicable PQC policies and regulations, with applicable city, state, and federal laws and regulations, and with applicable policies of the affiliated networks and systems.

Each person requesting service from a PQC Telecommunications and Networking technician for equipment owned by a person or entity other than PQC must acknowledge and accept the following liability release before the technician provides the requested service:

> By accepting technical support from the Telecommunications and Networking staff, users expressly waive all claims against PQC and its agents for any damages to my computer system or data that are incidental to the technical support rendered by Telecommunications and Networking. Users understand that the technical support received from Telecommunications and Networking may void manufacturer warranties and users understand that Telecommunications and Networking offers no verbal or written warranty, either expressed or implied, regarding the success of this technical support. Users understand that they have the right not to accept support from Telecommunications and Networking staff and to seek technical assistance elsewhere.