PROVIDENCE CHRISTIAN ACADEMY

Soli Deo Gloria

POLICY OF ACCEPTABLE USE OF INFORMATION TECHNOLOGY RESOURCES

Guiding Principles

In making information technology resources available to all members of the school community:

- *Providence Christian Academy* affirms its commitment to a scriptural standard of behavior.

- *Providence Christian Academy* respects individual privacy and intellectual property rights.

Under normal circumstances, school officials will not examine personal information transmitted over the network or stored on school-owned computers. However, the school reserves the right to monitor system resources, including activity and accounts, with or without notice, when:

- necessary to protect the integrity, security, or functionality of school computing resources

- an account or system is engaged in unusual or excessive activity

- it has good cause to believe that regulations, rules, or laws are being violated.

Additionally, the normal operation and maintenance of the school's computing resources requires the backup of data, the logging of activity, the monitoring of general usage patterns, and other such activities as may be necessary in order to provide desired services.

User Responsibilities

Access to computing resources and network capacity is a privilege to which all school faculty, staff and students are entitled. Access may be granted to other individuals affiliated with the school or school personnel, as situations warrant and with approval from the Director of Information Technology. Certain responsibilities correspond with that privilege, including those responsibilities listed below. Since no list can cover all possible circumstances, the spirit of this policy must be respected, namely: any action that hinders legitimate computer usage or invades the privacy of another person or institution is unacceptable.

Use of PCA Facilities

- Users must not abuse equipment and are asked to report any mistreatment or vandalism of computing or network facilities to PCA staff. If a user is found to be responsible for any damage he/she will be held accountable for repair or replacement costs. Food and beverages (including water) are prohibited in all PCA computer facilities, because of potential harm to equipment.

- Users shall relinquish the computer they are using if they are doing non-essential work when others are waiting for a computer to perform course-related activities. Game playing is prohibited at all times unless authorized by a PCA staff member.

- Users shall not install software, alter system files, or disconnect any cables on computers or other equipment.

- Users must respect all users and the staff of PCA as well as notices (such as those concerning hours of operation, printing, etc.) posted in PCA facilities.

Legal Usage

- Information technology resources may not be used for illegal or harmful purposes, including:

    - harassment of others
    - destruction or damage to equipment, software, or data
    - disruption or unauthorized monitoring of electronic communications

- Software is normally distributed under three kinds of licenses: proprietary, public distribution, and shareware. Unless otherwise indicated, users should assume that all software made available by PCA is proprietary and may not be legally copied.

- PCA will not knowingly provide support for software that a user possesses in violation of its license agreement. Consultants and staff may ask for proof of ownership before helping users with their software.

- PCA will not knowingly allow pirated software to be used on PCA computers. We will remove any suspect software loaded onto PCA computers or servers.

- PCA will not knowingly allow use of its resources for the illegal copying of digital media. Note: U.S. Copyright Law protects copyright owners from the unauthorized reproduction, adaptation, or distribution of sound recordings, including the unauthorized use of copyrighted mp3 files.

Ethical Usage

- Users shall not use information technology resources, including personally-owned computers connected to the school network, for non-education, unsanctioned, commercial activity.

- Users shall make no attempt to alter the condition or status of any computing network component in any manner.

- Users shall make no attempt to alter software, or to copy software intended only for execution.

- Users shall not interfere with, interrupt, or obstruct the ability of others to use the network or other PCA resources.

- Users shall not attempt to connect to a host via the network without explicit PCA permission.

- Users shall not provide, assist in, or gain unauthorized access to school computing or network resources.

- Users shall not attempt to circumvent or defeat computer or network security measures.

Security

- The school uses various measures to ensure the security of its computing resources. Users should be aware that the school cannot guarantee total security and should apply appropriate safeguards for their accounts, such as guarding their passwords and asking for password changes regularly (required for e-mail accounts), and logging out of computers when done.

- The default protection setting on PCA servers is that all files belong exclusively to their owners. Unless the owner changes the protection level, no file may be read, executed, or modified by users other than the owner. The only exception to this understanding is that designated members of the PCA staff may examine accounts or files of users to investigate security problems, possible abuse of the *Providence Christian Academy* computing system, or violations of regulations.

Account Usage

- Account holders shall only use their own personal accounts unless given permission by an authorized member of the faculty, administration, or professional staff to use one that is designated for a specific purpose or job. Account holders may not allow others to use their personal accounts. The person holding an account is responsible for its use, and all activity originating from that account, at all times.

- Account holders shall protect their passwords and keep them confidential. Passwords will be changed frequently. Any problem resulting from irresponsible use of a password (e.g., a password that can be easily guessed or oral or written dissemination of a password) may be treated as grounds for action against the account holder. Any attempt to determine the passwords of other users is strictly prohibited.

- Account holders shall not abuse any electronic mail, bulletin board, or communications system, either local or remote, by sending rude, obscene, or harassing messages (including chain letters) or by using these systems for non-essential purposes.

- Account holders shall identify themselves clearly and accurately in all electronic communications, i.e., no anonymous postings. Unofficial mass e-mailings (i.e., spam) are prohibited.

- Account holders shall only use their own files, those that have been designated as public, or those that have been made available to them with the knowledge and consent of the owner.

Personal Computer Usage

The following are responsibilities that are particularly applicable to those users that are permitted to attach their personal computer to PCA's network:

- No personal computers are permitted without administrative approval.

- Excessive or improper use of network resources that inhibits or interferes with use by others is prohibited and will be cause for action by PCA, which may include restricting, limiting, or disabling network access.

Enforcement

Violations of this Policy will be adjudicated, as deemed appropriate, and may include:

- Loss of computing privileges or disconnection from the network
- Prosecution under applicable civil or criminal laws