TELECOMMUNICATIONS / TECHNOLOGY

The Glen Rock School District is responsible for securing its computer network systems, including Internet services, to a reasonable and economically feasible degree against unauthorized access and/or abuse, while making them accessible for authorized and legitimate users. This responsibility includes informing users, both registered and unregistered, of expected standards of conduct and the disciplinary or legal consequences for not adhering to those standards. Any attempt to violate the provisions of this policy will result in disciplinary action, including but not limited to temporary revocation of user accounts, regardless of the success or failure of the attempt. Permanent revocations can result from disciplinary actions taken by the administrator called upon to investigate network abuses.

The users of the network are responsible for respecting and adhering to local, state, federal and international laws. Any attempt to break those laws through the use of the network may result in litigation against the offender by the proper authorities. If such an event should occur, this district will fully comply with the authorities to provide any information necessary for the litigation process.

The Glen Rock network and computing systems are expected to be used exclusively for education-related functions and applications. As the telecommunications systems manager has access to all files, including email files, users should have no expectation of privacy with respect to said files or email. Further, the Glen Rock Schools are obligated to cooperate fully with local, state or federal officials in any investigation concerning or relating to any email transmitted on or misuses of the network and computing systems.

SECTION 1: NETWORK AND COMPUTING SYSTEM SECURITY

A user of the network may be allowed to access only authorized networks or the computer systems attached to those networks. Therefore, the following are prohibited:

1.1 Using systems and/or networks in an attempt to gain unauthorized access to remote systems.

1.2 Using systems or networks to connect to other systems evading the restrictions of the local or remote system.

1.3 Decrypting system or user passwords.

1.4 Copying restricted files without authorization.

1.5 Duplicating materials protected by copyright, such as third-party software, without the express written permission of the copyright holder or without the proper license.

1.6 Attempting to "crash" network systems or programs.

1.7 Attempting to secure a higher level of privilege on network systems.

1.8 Willfully introducing computer "viruses," disruptive, or destructive programs into the organization network or into external networks.

SECTION 2: GENERAL COMPUTING POLICY

Once a user receives a user ID to be used to access the network and computer systems on that network, the user is solely responsible for all his/her actions while using that user ID. Therefore, the following actions are prohibited:

2.1 Applying for or acquiring a user ID under false pretenses.

2.2 Sharing a user ID with another person. If the user ID is shared, both the holder and the user of the user ID will be responsible for any abuse.

2.3 Deleting, examining, copying, or modifying files and/or data belonging to other users without their prior consent.

2.4 Using facilities and/or services for unauthorized commercial purposes.

2.5 Any unauthorized, deliberate action which damages or disrupts a computing system or network, alters its normal performance or causes a malfunction regardless of system location or time duration.

2.6 Attempting to log onto any system as a system manager or as a higher level than assigned.

SECTION 3: INTERNET SERVICES

The use of the Internet is a privilege, not a right. Inappropriate use, including any violation of these conditions and rules, may result in cancellation of the privilege, a disciplinary action by the Glen Rock Board of Education and/or civil and/or criminal penalties. The board of education has the authority to determine acceptable use.

3.1 Acceptable Use

3.1.1 The purpose of the Internet is to facilitate communications in support of research and education by providing access to unique resources and an opportunity for collaborative work. To remain eligible as a user, the use of any account must be in support of and consistent with the educational objectives of the district. Access to the Internet is made possible through an appropriate provider to be designated by the Glen Rock Board of Education at its sole discretion. All users must comply with contractual provisions and rules of usage of the provider. In addition, all users of the Internet must comply with existing rules and acceptable use policies of the Glen Rock Board of Education. All pupils shall immediately report to their teacher the receipt of any unsolicited, offensive, or inappropriate electronic mail or other communications. Any teacher who receives such a report from a pupil must immediately report the incident to the principal, who shall then report it to the chief school administrator, and the appropriate actions shall be taken, including, but not limited to notifying the authorities.

3.1.2 Storage and/or transmission of any material in violation of any United States or state regulation is prohibited. This includes, but is not limited to, copyrighting material, threatening or obscene material, or material protected by trade secret.

3.1.3 Use for commercial activities is not acceptable.

3.2 Monitoring

The Glen Rock Board of Education reserves the right to review any material and to monitor fileserver space in order to make determinations on whether specific uses of the network are inappropriate. Users of the district's telecommunications system and the Internet should not expect that files stored on the district's servers will be private or that incoming, out-going or stored electronic mails will be private. However, if strict security and/or confidentiality is of concern it is recommended that the user not utilize the Internet connections provided by the Glen Rock Board of Education.

3.3 Network Etiquette

All users are expected to abide by the generally accepted rules of network etiquette. Therefore, the following are prohibited:

3.3.1 Engaging in any activities which are prohibited under state and/or federal law or code, including, but not limited to, copyright infringement.

3.3.2 Using abusive and/or inappropriate language in messages or postings.

3.3.3 Revealing personal addresses, phone numbers, credit card information or other personal information of user, fellow pupils or colleagues.

3.3.4.1 Using the network in such a way that the use of the network by others would be disrupted. The systems manager will be responsible for overseeing systems resource allocation.

3.3.5 Arranging personal meetings over the Internet.

3.3.6 Sending or displaying messages or pictures that are obscene, libelous, hateful, discriminatory, or sexually harassing, as determined by the Glen Rock Board of Education.

3.3.7 Sending any communication for the purpose of promoting or participating in violence or illegal activities.

3.4 No Warranties

The Board of Education makes no warranties of any kind, whether express or implied, for the service it is providing or the materials and information obtained off of the district's telecommunications system and/or the Internet. It will not be responsible for any damages a user suffers. This includes loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by the negligence of the Glen Rock Board of Education or by the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The board specifically denies any responsibility for the accuracy or quality of information obtained through its services. All users need to consider the source of any information obtained, and consider how valid that information may be.

3.5 Security

Security on any computer system is a high priority, especially when the system involves many users. Any user identified as a security risk by the systems manager for having a

3.5 Security (continued)
history of problems with other computer systems may be denied access to the Internet. Any user who encounters a security problem on the Internet must notify the systems manager without demonstrating the problem to other users.

All users must protect their password to ensure system security and their own privilege and ability to maintain continued use of the system. Therefore, the following are prohibited:
3.5.1 Using another individual's account for any purpose.

3.5.2 Giving your account number to another individual for his/her use.

3.6 Vandalism and Harassment
3.6.1 Vandalism and harassment will result in cancellation of user privileges and prosecution to the fullest extent of the law.

3.6.2 Harassment is defined as the persistent annoyance of another user, or the interference with another user's work. Harassment includes, but is not limited to, the sending of unwanted email.

3.7 Procedures for Use
3.7.1 Pupil users must always get permission from their instructors and/or librarian before using computers and/or the network.

3.7.2 Users shall not play games or use the computer resources for other non-academic activities when other users require the system for academic purposes. In addition, users shall neither waste nor take supplies such as paper, printer ribbons, and diskettes.

3.8 Encounter of Controversial Material
Users may encounter material which is controversial and which users, parents, teachers or administrator may consider inappropriate or offensive. It is impossible, on a global network, to control effectively the content of data and an industrious user may discover controversial material. Users are prohibited from initiating access to such material. Any decision by the Glen Rock Board of Education to restrict access to Internet material shall not be deemed to impose any duty on the Glen Rock Board of Education to regulate the content of material on the Internet.

SECTION 4: EMAIL (ELECTRONIC MAIL)

Email is an electronic message sent by or to a user in correspondence with another person having email access. Email is not guaranteed to be private; the systems manager will have access to all email in the system. Messages relating to or in support of inappropriate activities will be reported to the administrator and may result in the suspension or loss of user privileges. Illegal activities will be reported immediately to the chief school administrator and shall be reported to the appropriate authorities, potentially resulting in civil and/or criminal penalties.

4.1 Users are expected to remove old messages in a timely fashion. After giving notice, the system manager will remove old messages from an account if the user does not do so.

4.2 A cancelled account will not retain its email.

4.3 The user's name and user ID are included in the header of each email message sent. The user is responsible for all email from his/her user ID. Therefore, the following are prohibited:

4.3.1 Forging or attempting to forge email messages.

4.3.2 Reading, deleting, copying, modifying or viewing other users' email without permission or attempting to do so.

4.3.3 Sending or attempting to send harassing, obscene and/or other threatening email to another user.

4.3.4 Sending or attempting to send unsolicited junk mail ("spamming" or "mailbombing"), for-profit messages, or chain letters.

4.3.5 Altering or attempting to alter the identifying headers of postings to conceal the sender's email address.

4.3.6 Sending email to any user who has specifically requested not to receive it.

Approved: August 25, 1997
Revised: January 11, 1999, March 28, 2005