GLEN ROCK BOARD OF EDUCATION **FILE CODE: 6142.10***
Glen Rock, NJ 07452 **Policy**

TELECOMMUNICATIONS / TECHNOLOGY

The Glen Rock Board of Education is committed to the development and establishment of a quality, equitable and cost-effective electronic telecommunications system, including Internet services. The system's sole purpose shall be for the advancement and promotion of learning and teaching. Glen Rock will not disclose or share any information collected about individual pupils with third parties accept as required by law. While there are many valuable uses of the Internet and the district's telecommunications system, there is the possibility of encountering offensive or inappropriate material on the Internet, despite the Glen Rock Board of Education's efforts to prohibit and guard against access to such material. However, the benefits of a student's use of the district's telecommunications system and the Internet far outweigh these potential detriments.

The district's system will be used to provide local, state-wide, national, and global communications opportunities for staff and students. Beginning February 13, 2015, the district shall incorporate instruction for all pupils as appropriate on the use of social media as part of the Common Core Curriculum Standards.

Educational technology shall be infused into the district curriculum to maximize student achievement of the Common Core Curriculum Content Standards.

It is the policy of the district to establish safe and effective methods for student and staff users of the district's technological resources and to:

A. Prevent user access over its computer network to, or transmission of, inappropriate material via Internet, electronic mail, or other forms of direct electronic communications including social media;

B. Prevent unauthorized access and other unlawful online activity;

C. Prevent unauthorized online disclosure, use, or dissemination of personal identification information of minors; and

D. Comply with the Children's Internet Protection Act (CIPA) and the Children's Online Privacy Protection Act (COPPA).

Limitation of Liability

The Internet constitutes an unregulated collection of resources that changes constantly, so it is not possible to totally predict or control the resources that users may locate. The board cannot guarantee the accuracy of the information or the appropriateness of materials that a user may encounter. Furthermore, the board shall not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. Nor shall the board be responsible for financial obligations arising through the unauthorized use of the system.

District Rights and Responsibilities

The computer system is the property of the district, and all computer software and hardware belong to it. Therefore, the district retains the right to monitor all access and use of the network and Internet.

TECHNOLOGY (continued)

District Rights and Responsibilities

The board designates the chief school administrator as the coordinator of the district system. He/she shall recommend to the board of education qualified staff persons to ensure provision of individual and class accounts necessary for access to the Internet, designation of resources for disk usage on the system, establishment of a document retention schedule, establishment of a virus protection process and coordination of other activities as required to maintain the system. The chief school administrator shall establish administrative regulations for the use of the district's system. These regulations shall be consistent with district policy and pertinent state and federal law. These regulations must be reviewed at least annually to reflect changes in telecommunications these are to be overseen by the Network Administrator.

This policy shall govern all use of the system. Failure to abide by district policy and administrative regulations governing use of the district's system may result in the suspension and/or revocation of system access as well as civil and/or criminal penalties. Pupil violations may result in discipline (see Policy 5131 Conduct/Discipline.) Staff violations may also result in discipline. Additionally, a pupil's parent(s) or legal guardian(s) shall be responsible for any damages which the pupil causes or any legal liability that results from the pupil's use of the district's telecommunications system and the Internet.

Parental Notification and Responsibility

The chief school administrator shall ensure that parents/guardians are notified about the district network and the rules governing its use. No pupil will be permitted to use the district's telecommunications system unless and until the pupil and his/her parents (if the pupil is less than 18 years old) sign the district's Acceptable Use Policy (6142.10-E1) which acknowledges that:

A. The pupil and his/her parent, if applicable, have read and understand this policy and the accompanying regulation;

B. The pupil will be held accountable for all of his/her network and Internet activities;

C. The pupil is expected to comply with the district's policy and regulation and all federal, state and local laws governing Internet use; and

D. The pupil and his/her parent shall indemnify and hold harmless the Glen Rock Board of Education, its members, agents, servants and employees from any and all liability relating to the pupil's use of the district's telecommunications system, ~~or~~ the Internet or social/other media.

Parents/guardians who do not wish their child(ren) to have access to the Internet must notify the principal in writing.

Additionally, all teachers are required to discuss the technology policy and regulation with each of his/her classes and sign an acknowledgment that they have had such a discussion with his/her classes and the date(s) on which said discussions occurred.

World Wide Web

All pupils and employees of the board shall have access to the Web through the district's networked. The board shall ensure the acquisition and installation of blocking/filtering software to deny access to certain areas of the Internet. An agreement shall be required. To deny a child access, parents/guardians must notify the building principal in writing.

TECHNOLOGY (continued)

Social Media for Educational Purposes In the Middle School and High School
Social media may be used for appropriate educational purposes if it is overseen by a staff member and approved by the building principal.

Compliance With CIPA and COPPA

A. Filters Blocking Access to Inappropriate Material
To the extent practical, technology protection measures (or "Internet filters") shall be used to block or filter Internet, or other forms of electronic communications, access to inappropriate information. Specifically, as required by the Children's Internet Protection Act, blocking shall be applied to visual depictions of material deemed obscene or child pornography, or to any material deemed harmful to minors.

Subject to staff supervision, technology protection measures may be disabled or, in the case of minors, minimized only for bona fide research or other lawful purposes.

B. Privacy
The district shall observe all privacy requirements as dictated by COPPA.

C. Inappropriate Network Usage
To the extent practical, steps shall be taken to promote the safety and security of users of the school district online computer network.

Specifically, as required by the Children's Internet Protection Act, prevention of inappropriate network usage includes:

1. Unauthorized access, including so-called "hacking," and other unlawful activities; and

2. Unauthorized disclosure, use, and dissemination of personal identification information regarding minors.

D. Education, Supervision and Monitoring
It shall be the responsibility of all members of the school district staff to educate, supervise and monitor usage of the online computer network and access to the Internet in accordance with this policy and the Children's Internet protection Act. Procedures for the disabling or otherwise modifying any technology protection measures shall be the responsibility of the chief school administrator or his or her designee.

The chief school administrator or his or her designee shall ensure that students and staff who use the school internet facilities receive appropriate training including the following:

1. The district established standards for the acceptable use of the internet;

2. Internet safety rules;

3. Rules for limited supervised access to and appropriate behavioral expectations for use of online resources, social network websites, and chat rooms;

4. Cyberbullying (board policy 5131.2 Harassment, Intimidation and Bullying) awareness and response.

Pupil use of the Internet shall be supervised by qualified staff.

TECHNOLOGY (continued)

E. Pupil Safety Practices

Pupils shall not post personal contact information about themselves or others. ~~Nor shall~~ Pupils shall not engage in any kind of personal contact with individuals they meet online. Attempts at contact from such individuals shall be reported immediately to the staff person monitoring that child's access to the Internet. Personal contact information includes but is not limited to names, home/school/work addresses, telephone numbers, or personal photographs.

Email Accounts For Pupils

Pupils K-2 shall be granted email access through classroom accounts if requested by a teacher. To deny a child access to a classroom account, parents/guardians must notify the building principal in writing.

Pupils in grades K-12 have individual accounts. An individual account for any such pupil shall require an agreement signed by the pupil and his/her parent/guardian.

Individual Email Accounts for District Employees

District employees shall be provided with an individual account ~~and dial-up access to the system~~. An agreement shall not be required, but the rules and regulations will be discussed with all staff. (Policies 4119.27 and 4219.27 Use of Internet Social Networks and Other Forms of Electronic Communication.).

District Web Site

The board authorizes the chief school administrator to establish and maintain a district web site. The purpose of the web site will be to inform the district educational community of district programs, policies and practices.

Individual schools and classes may also establish web sites that include information on the activities of that school or class. The building principal shall oversee these web sites. The chief school administrator shall publish and disseminate guidelines on acceptable material for these web sites. The chief school administrator and building principals shall also ensure that district and school web sites do not disclose personally identifiable information about pupils without prior written consent from parents/guardians. Consent shall be obtained on the form developed by the state department of education. "Personally identifiable information" shall include but not be limited to pupil names, photos, addresses, email addresses, phone numbers, social security numbers, ~~instant message addresses,~~ and locations and times of class trips.

Prohibited Activities

Users shall not attempt to gain unauthorized access to the district system or to any other computer system through the district system, nor shall they go beyond their authorized access. This includes attempting to log in through another individual's account or accessing another's files.

Users shall not deliberately attempt to disrupt the district's computer system performance or destroy data by spreading computer viruses, worms, "Trojan Horses," trap door program codes or any similar product that can damage computer systems, firewalls, servers or network systems.

Users shall not use the district system to engage in illegal activities.

Users shall not access material that is profane or obscene, that advocates illegal acts, or that advocates violence or hate. Inadvertent access to such material should be reported immediately to the supervising staff person.

TECHNOLOGY (continued)

Prohibited Activities (continued)
Users shall not perform any acts on the district computer system or on the district-supplied computers that are not related to their work at Glen Rock.

Prohibited Language
Prohibited language applies, but is not limited to, public messages, private messages, and material posted on web pages.

Users shall not send or receive messages that contain obscene, profane, lewd, vulgar, rude, inflammatory, or threatening language. Inadvertent access to such material should be reported immediately to the building principal.

Users shall not use the system to spread messages data, images or other electronic resources that can reasonably be interpreted as harassing, discriminatory or defamatory.

System Security
Users are responsible for their accounts and should take all reasonable precautions to prevent unauthorized access to them. In no case should a user provide his/her password to another individual.

Users shall immediately notify the supervising staff person or data processing department if they detect a possible security problem. Users shall not access the system for the purpose of searching for security problems.

Users shall not install or download software or other applications.

Users shall immediately notify the supervising staff person if they detect a possible security problem. Users shall not access the system for the purpose of searching for security problems.

Intellectual Property and Plagiarism
Because certain works found on the Internet are protected by copyright, trademark, and other forms of intellectual property, pupils will either request permission from the owner of the intellectual property rights prior to using any materials obtained on the Internet, or the pupils will consult with the administration to determine whether the materials may be used without receiving permission based on certain exceptions to intellectual property rights as set forth in the relevant laws. Committing plagiarism is subject to discipline as per the Student Handbook Code of Conduct.

Users will be held personally liable for any of their own actions that violate another party's intellectual property rights. District practices on plagiarism will govern the use of materials accessed through the Internet. Teachers will instruct students as to the definition of plagiarism and the proper method to cite to materials.

Legal References:	
N.J.S.A. 2A:38A-1 et seq.	Computer System
N.J.S.A. 2C:20-25	Computer Related Theft
N.J.S.A.18A:7A-10 et seq.	New Jersey Quality Sincle Accountability Continuum for evaluating education
N.J.S.A. 18A:36-35	School internet websites; disclosure of certain student information prohibited
N.J.S.A.18A:36-39	Notification by school to certain persons using certain electronic devices; fine
N.J.A.C. 6A:30-1.1 et seq.	Evaluation of the Performance of School Districts

TECHNOLOGY (continued)

Legal References:(continued)

17 U.S.C. 101	United States Copyright Law
47 CFR 54.503(d)	Competitive bidding; gift restrictions
47 U.S.C. 254(h)	Children's Internet Protection Act
NJ P.L.2013, c.44.	Anti Big Brother Act

State in re T..L.O 94 N.J. 331 (1983) reversed on other grounds N.J. v. T.L.O. 569 U.S. 325 (1985)

O'Connor v. Ortega 480 U.S. 709 (1987)

COPPA

Anti-Bullying Rights Act

No Child Left Behind Act of 2001 Pub. L. 107-110, 20 U.S.C.A. 6301 et seq.

Cross References:

*1111	District publications
*3514	Equipment
3543	Office services
4118.2/4218.2	Freedom of speech (staff)
*5114	Suspension and expulsion
*5124	Reporting to parents/guardians
*5131	Conduct/discipline
*5131.5	Vandalism/violence
*5142	Pupil safety
5145.2	Freedom of speech/expression (students)
*6144	Controversial issues
*6145.3	Publications
6161	Equipment, books and materials

*Indicates policy is included in the Critical Policy Reference Manual.

Key Words
Acceptable Use, Blocking/Filtering Software, Email, Internet, Technology, Web Site, World Wide Web

Approved: February 3, 1997
Revised: January 11, 1999, April 12, 2004, July 11, 2011, March 21, 2013. June 23, 2014,