DEMAREST BOARD OF EDUCATION **FILE CODE: 6142.10***
Demarest, NJ 07627 **Policy**

TELECOMMUNICATIONS/TECHNOLOGY

The board shall develop a technology plan that effectively uses electronic communication to advance and promote learning and teaching. This system of technology shall be used to provide local, statewide, national and global communications opportunities for staff and pupils. Educational technology shall be infused into the district curriculum to maximize pupil achievement of the Core Curriculum Content Standards.

Educational technology shall be infused into the district curriculum to maximize pupil achievement of the Core Curriculum Content Standards. Beginning in the 2014/2015 school year, the district shall incorporate instruction on the responsible use of social media into the technology education curriculum for students in grades 4 through 8 as part of the implementation of the core curriculum standards.

It is the policy of the district to establish safe and effective methods for pupil 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;

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).

Definitions

For the purposes of this policy, the following definitions shall apply:

1. Computer Network/Computers consist of any school managed or owned computer equipment or systems, including, but not limited to, networks, hard drives, servers, peripherals, printers, networking systems, devices, modems, all electronic documents, video, voice and data networks, routers, storage devices, and classrooms equipped with such. Computer Network/Computers shall also include electronic communications which shall be defined as and include the use of information systems in the communicating, posting, or obtaining of information or materials by way of electronic mail, bulletin boards, Internet, or other such electronic tools.

2. User is any individual, with or without authorization, who utilizes the district's computing system from any location.

Compliance With CIPA

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.

TECHNOLOGY (continued)

Compliance With CIPA

A. Filters Blocking Access to Inappropriate Material (continued)
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. 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 when using electronic mail, chat rooms, instant messaging, and other forms of direct electronic communications.

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.

C. 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 pupils 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.

Standards for the Promotion of Online Safety for Pupils

While the Internet offers a variety of opportunities to enhance pupils' educational experiences, there are certain risks associated with the Internet created by other users. Pupils are required to adhere to the following guidelines regarding safety. Any individual who fails to adhere to these guidelines will have his/her network privileges revoked.

1. Users are prohibited from disclosing personal information such as addresses, phone numbers, pictures, or the name and location of the school without the permission of a teacher and a parent.

TECHNOLOGY (continued)

Standards for the Promotion of Online Safety for Pupils (continued)

2. Users are obligated to disclose to a teacher or parent any information or electronic messages which make them uncomfortable.

3. Users shall never meet in person with someone they have met online without first receiving permission from a parent. The board does not condone such meetings and strongly suggests that they do not occur.

4 Users shall report any security problems, such as a gap in system or network security, to a teacher or system administrator.

5. Users shall set a password for their account to protect it from unauthorized use. The password should be difficult to guess and should be changed on a regular basis to assure the continued security of the account. Users should never divulge their passwords and will be held accountable for the consequences of intentionally or negligently disseminating this information.

Acceptable Use Of The Internet

The board recognizes that telecommunications and other new technologies will shift the manner in which information is accessed, communicated, and transferred. These new technologies will alter the nature of teaching and learning. Access to telecommunications will allow pupils and employees to explore databases, libraries, Internet sites, bulletin boards and the like while exchanging information with individuals throughout the world. The board supports access by pupils and employees to these information sources and the potential they have to enhance pupils' educational experiences, but it reserves the right to limit use of these new technologies during school hours and on school premises to legitimate educational purposes. At all other times, the board demands that users utilize the computer network in a responsible manner and in accordance with this policy.

The board also recognizes that telecommunications will allow pupils access to information sources that have not been pre-screened by educators using board approved standards. While the board will make its best efforts to monitor use of school computer networks/computers, the board cannot monitor users at all times and cannot guarantee that users will not access inappropriate materials**,** especially when access is from a site off campus. The board therefore adopts the following standards of conduct for the use of computer network/computers, including electronic mail communications, to which all users are expected to adhere, and declares unethical, unacceptable and illegal behavior in violation of these standards, and said behavior will serve as just cause for taking disciplinary action, limiting or revoking network access privileges, and/or instituting legal action.

The board provides access to computer network/computers for educational purposes only, and, for employees, for purposes related to job performance. The board retains the right to restrict or to terminate access to the computer network/computers at any time, for any reason. The board retains the right to have district personnel monitor network activity, in any form necessary, to maintain the integrity of the network and to ensure its proper use.

Standards for Use of Computer Networks

It is understood that computer networked services are provided exclusively for educational purposes. Educational purposes are those that are related to or necessary to prepare for or to complete lessons or classroom assignments, and, for employees, those purposes related to job performance. Users will adhere to the standard of conduct required in the classroom and will follow the regulations posted in the computer lab. Users are prohibited from engaging in the

TECHNOLOGY (continued)

Standards for Use of Computer Networks (continued)

following conduct and shall be subject to discipline and/or legal action for such conduct:

1. Using the computer network/computers for illegal activities or in support of illegal activities. Illegal activities are defined as activities which violate federal, state, and local laws or regulations.

2. Using the computer network/computers in a way that violates existing district policy.

3. Using the computer network/computers for obscene purposes or to obtain or transmit obscene materials. Obscene materials are those that appeal to the prurient interest, depict sexual conduct in a patently offensive way, and lack serious literary, artistic, or scientific value.

4. Using the computer network/computers to send or display lewd, indecent, or vulgar speech or materials.

5. Using the computer network/computers to send or display harassing, demeaning, or offensive speech or materials.

6. Using the computer network/computers to engage in activities that could materially or substantially interfere with the operation of the school, the school's educational mission, or other pupils' rights.

7. Using the computer network/computers to violate copyrights, trademarks, an individual's right of publicity, any form of intellectual property, license agreements, or other contracts.

8. Displaying any personally identifiable information about pupils including name, address, photographs, social security number, or other personal characteristics that would make the pupil easily identifiable without obtaining prior parental consent. Consent shall be obtained on the form developed by the state department of education. "Personally identifiable information" refers to pupil names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips.

9. Using the computer networks/computers in a manner that:
   a. Intentionally disrupts network traffic or crashes the network;

   b. Degrades or disrupts equipment or system performance. Examples of conduct that degrade or disrupt equipment or system performance include, but are not limited to, the following activities: utilizing shared computing resources for excessive game playing or other trivial applications; sending unnecessary or excessive mail or messages; printing of excessive copies of documents, files, images or data; deliberately running grossly inefficient programs when more efficient choices are available; creating, sending, or forwarding electronic chain letters;

   c. Uses the computing resources of the school district for commercial purposes, financial gain, or fraud;

   d. Steals data or other intellectual property;

   e. Gains or seeks unauthorized access to files of others or vandalizes the data of another user;

TECHNOLOGY (continued)

f. Forges electronic mail messages or uses an account owned by others; and/or creates an account under false/identity theft.

Standards for Use of Computer Networks (continued)

g. Invades the privacy of others. Users will not use the network to obtain private information about others, post private information about another person, or re-post a message that was sent to them privately without permission of the person who sent the message;

h. Posts anonymous messages;

i. Possesses any data which is in violation of this policy; and/or

j. Engages in other activities that do not advance the educational purposes for which the computer network/computers are provided.

k. Uses outside software without the prior approval of the school's technology coordinator or system administrator.

Off school premises, users may utilize the computer network for legitimate, non-education related reasons. However, users are expected to adhere to this policy in all other regards, and specifically, shall adhere to the user guidelines set forth above.

Users will be personally charged for any unauthorized costs incurred in their use of the computer network/computers and held responsible for any damages caused by their intentional misuse of the computer network/computer equipment.

Users are required to report any evidence of a violation of these rules to school authorities and employees are expected to ensure to the best of their abilities that pupils use the computer network/computers in accordance with this policy.

The district will fully cooperate with any local, state or federal agency in any investigation concerning or relating to misuse of the district's computer network/computers.

Aside from this policy, use of the computer network/computers by pupils and employees will be governed by the district's existing policies and, for employees, the existing Collective Bargaining Agreement specifically as it relates to professional conduct.

Any violation of district policy and rules may result in a loss of district-provided access to the Internet. Violations may result in additional disciplinary action, including suspension and expulsion. When applicable, law enforcement agencies will be contacted regarding potential illegal activities. Specifically, individuals violating this policy shall be subject to appropriate discipline which could include, but which is not limited to,

a. Use of network only under direct supervision;
b. Suspension of network privileges;
c. Revocation of network privileges;
d. Suspension of computer privileges;
e. Revocation of computer privileges;
f. For pupils, suspension or expulsion from school;
g. For employees, letters of reprimand, increment withholding, loss of employment; and/or
h. Legal action and prosecution by the authorities.

TECHNOLOGY (continued)

Privacy
Individuals should have no expectation of privacy with respect to their files on board provided computer network/computers. All data stored or transmitted or accessed by users, including E-mail, can and will be monitored by the board.

Due Process
In the event there is an allegation that a pupil has violated the Acceptable Use Policy, that pupil will be provided with a written notice of the alleged violation and an opportunity to present an explanation before a district administrator. A hearing will be provided when required by district policy or the applicable statutes and regulations governing discipline of pupils.

Employee violations of the Acceptable Use Policy will be handled in accordance with district policy and the current Collective Bargaining Agreement.

Intellectual Property and Plagiarism
Because certain works found on the Internet are protected by copyright, trademark, and other forms of intellectual property, employees will either request permission from the owner of the intellectual property rights prior to using any materials obtained on the Internet, or the employee 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. Teachers will instruct pupils to adhere to the same guidelines.

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 pupils as to the definition of plagiarism and the proper method to cite to materials.

Responsibility for Damage Suffered
The Demarest Public School District makes no warranties of any kind, expressed or implied, for the Internet access it provides. The district will not be responsible for any damage users suffer including, but not limited to, loss of data or interruption of service. The district will also not be responsible for the accuracy or quality of the information obtained through or stored on the system. The board will not be responsible for financial obligations arising from the unauthorized use of the system.

District Web Site
The chief school administrator shall publish and disseminate guidelines on acceptable material for district web sites. The chief school administrator 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" refers to pupil names, photos, addresses, e-mail addresses, phone numbers and locations and times of class trips.

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 Consent and Release Form which acknowledges that:
A. The pupil and his/her parent, if applicable, have read and understand this policy and the

TECHNOLOGY (continued)

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 Demarest Board of

Parental Notification and Responsibility (continued)

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.

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

Consent Requirement

No pupil shall be allowed to use the district-provided computer network unless they have filed an executed consent form with the principal. Guests to the school must also sign a consent form. Consent forms are available from the main office. Anyone using the system without first executing a consent form will be deemed to have consented to the principles embodied in this policy.

Policy Development

The district Internet Safety and Technology policy shall be adopted and revised through a procedure that includes reasonable public notice and at least one public hearing.

Implementation

The chief school administrator shall prepare regulations to implement this policy.

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-11	Annual report of local school district; contents; annual report of commissioner; report on improvement of basic skills
	N.J.S.A. 18A:36-35	School internet websites; disclosure of certain pupil information prohibited
	N.J.A.C. 6A:24-1.1 et seq.	*Urban Education Reform in the Abbott Districts*
	See particularly:	
	N.J.A.C. 6A:24-1.4, 2.2, 4.1, 6.1	
	N.J.A.C. 6A:30-1.1 et seq.	Evaluation of the Performance of School Districts
	17 U.S.C. 101	United States Copyright Law
	47 U.S.C. 254(h)	Children's Internet Protection Act
	N.J. v. T.L.O. 469 U.S. 325 (1985)	
	P.L.2013, c.257	***Social Media Use***
	O'Connor v. Ortega 480 U.S. 709 (1987)	
	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

TECHNOLOGY (continued)

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 (pupils)
*6144	Controversial issues
*6145.3	Publications

Cross References: (continued)

6161	Equipment, books and materials

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

Key Words

Acceptable Use, Blocking/Filtering Software, E-mail, Internet, Technology, Web Site, World Wide Web, ***Social Media Use***

Approved: May 2002
Revised: July 22, 2003, March 28, 2006, February 27, 2007, February 26, 2013, March 25, 2014