THE NEWARK PUBLIC SCHOOLS
Newark, New Jersey
POLICY

FILE CODE: 6142.10

TECHNOLOGY

The Newark Public Schools (the "District") 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.

ACCEPTABLE USE OF THE INTERNET (AUP)

Purpose

To support its commitment to providing avenues of access to the universe of information available, the District's system of electronic communication shall include access to the Internet for pupils and staff.

The District is committed to the use of telecommunication networks in a responsible, efficient, courteous and legal manner. Internet access and other on-line services, provided to students and teachers, offer a multitude of global resources. Our goal in providing these services is to enhance the educational development of our students.

Acceptable uses of telecommunications are devoted to activities that support teaching and learning. The use of the District's computer network is limited to the exchange of academic information, research, career and professional development activities consistent with the mission of the District.

In support of the District's goal, users must agree to this policy as a condition of receiving Internet access. Usage is a privilege, not a right, and can be revoked at any time.

Limitation of Liability

The Internet constitutes an unregulated collection of resources that change constantly, so it is not possible to totally predict or control the resources that users may locate. The District cannot guarantee the accuracy of the information or the appropriateness of materials that a user may encounter. Furthermore, the District 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 District 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 to and use of the Internet.

The Chief Information Officer is the coordinator of the District system. He/she shall recommend to

TECHNOLOGY (continued)

the State District Superintendent qualified staff persons to ensure the provision of individual and class accounts necessary for access to the Internet, designation of quotas 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.

Each principal shall work with the site-based Technology Coordinator to maintain the District system in his/her building by approving all activities for that building; ensuring that teachers receive proper training in the use of the system; ensuring that pupils are adequately supervised when using the system; maintaining executed user agreements; and interpreting this acceptable use policy at the building level.

Access to the System

This acceptable use policy shall govern all use of the system. Sanctions for pupil misuse of the system shall be included in the disciplinary code for pupils, as set out in regulations for policy 5131.

Conduct/discipline

Employee misuse may result in appropriate discipline in accordance with the collective bargaining agreement and applicable laws and regulations.

The Director of Network Services shall ensure the acquisition and installation of blocking/ filtering software to deny access to certain areas of the Internet.

World Wide Web

All pupils and employees of the District shall have access to the Web through the District's networked or stand alone computers. An agreement shall be required. To deny a child access, parents/ guardians must notify the building principal in writing.

Individual E-mail Accounts for District Employees

1. District employees shall be provided with an individual account and access to the system. An agreement shall not be required.
2. The District computer system and the contents thereof are the property of the District.
3. E-mail is provided for the purpose of exchanging information consistent with the mission of the District. E-mail messaging on the District's computer system is intended for official business.
4. The information on the network belongs to the District. The District reserves the right to monitor messaging on the system to the extent permissible by law.
5. All correspondence protocols observed in the flow of paper communication must be similarly adhered to in E-mail transactions. Appropriate approvals of correspondence must take place before E-mail is sent to recipients.
6. Solicitation for charity donations and the selling of any products or services via E-mail is prohibited.
7. Non-essential announcements such as office greetings and general notifications (without appropriate approval) should not be posted on District E-mail.
8. Users must not post chain letters or engage in “spamming.” Spamming is the sending of an annoying and unnecessary message to a large number of people.

TECHNOLOGY (continued)

9. While engaged in activities on the District computer network, users are prohibited from transmitting E-mail to others that includes material that is vulgar, rude, obscene, pornographic, inflammatory, threatening, harassing, disrespectful or which uses sexually explicit language.
10. Users should not expect their E-mail communications to be private, and should not use District e-mail for confidential matters that are not intended for public disclosure.
11. E-mail is provided for the purpose of exchanging information consistent with the mission of the District.
12. Unauthorized attempt to read, delete, copy or modify e-mail of other users is prohibited.
13. All users must adhere to the same standards for communicating online that are expected in the classroom and that are consistent with District policies, regulations and procedures.
14. The use of clip art and backdrops consume an inordinate amount of computer system space and therefore such use is discouraged unless essential to the message.

Supervision of Pupils

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

District Web Site

The Director of Communications shall establish and maintain a District web site. The purpose of the web site is to inform the District educational community of District programs, policies and practices, from individual schools.

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 Director of Communications shall publish and disseminate guidelines on acceptable material for these web sites. The Director of Communications 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 State District Superintendent or designee shall ensure that parents/guardians are notified about the District network and the rules governing its use. Parents/guardians shall sign an agreement to allow their child(ren) to have an individual account. Parents/guardians who do not wish their child(ren) to have access to the Internet must notify the principal in writing.

Pupil Internet Safety Policy

It is the responsibility of the school staff to educate and provide ongoing guidance for pupils on personal safety practices, appropriate on-line behavior, cyberbullying awareness and response, and effective techniques for identifying and evaluating information and its sources. School staff shall be required to supervise and monitor appropriate usage of the online computer network and access to

TECHNOLOGY (continued)

the Internet in accordance with this policy.

No user may post personal contact information about themselves or others. 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.

Prohibited Activities

Unacceptable uses of the Districts' computer network accounts and Internet resources include, but are not limited to, the following:

1. Users may not use the NPS computer network to access, send, post, transmit, distribute, publish, display, download, print, or store false or defamatory information about a person or organization, abusive, pornographic, obscene, or offensive materials, images, or statements that advocate hate, violence, or harassment and discrimination towards others or to harass another person or engage in personal attacks.
2. 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.
3. Any speech that is considered inappropriate in the classroom should not be posted online whether in school or at home.
4. Users may not use the NPS computer network to engage in any illegal act or action that violates local, state or federal laws.
5. Users must not tamper with, modify, or change the District’s system, software, hardware, or wiring or use the network in any way that would disrupt the uses of the network by others.
6. Users shall not plagiarize material that is available on the Internet. Plagiarism is presenting another's ideas/words as one's own.
7. Users may not use the NPS computer network for private or commercial business use, political or religious purposes.
8. Users may not use the NPS computer network to advertise goods and services, or to purchase goods and services for personal use.
9. The downloading and storage of files, which consume excessive system resources, is strictly prohibited.
10. 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 someone else’s account or accessing someone else’s files.
11. 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.

System Security

Security on any computer system is a high priority, especially when the system involves many users. Keeping this in mind, all users must adhere to the following.

TECHNOLOGY (continued)

1. Users are responsible for their individual accounts and should take serious precautions to prevent others from being able to use their accounts. Attempts to log on as any other user will result in cancellation of user privileges.
2. Under no conditions or circumstances should users give passwords to other individuals or sign other users onto their account.
3. Vandalism will result in cancellation of privileges and possible disciplinary or legal action. Vandalism is defined as any malicious or intentional attempt to harm or destroy data of another user, the destruction of computer equipment or other property, the theft or defacing of computer equipment. This also includes the intentional uploading or creation of computer viruses when using the Internet.
4. Distribution of personal information over the Internet is strictly prohibited.
5. Users who are identified as a security risk or having a history of problems with other computer systems will be denied access to the Internet.
6. Students should never agree to meet in person with anyone they have met online unless they first have the approval of a parent or guardian.
7. A student's parent or guardian should instruct the student if there are additional materials that access to would be inappropriate. The District expects students to follow parent or guardian's guidance regarding such material.
8. Users shall immediately notify the supervising staff person, or the technology coordinator if they detect a possible security problem. Users shall not access the system solely for the purpose of searching for security problems.
9. Users shall not install or download software or other applications without permission of supervising staff person.

Software

1. Users are responsible to take all reasonable precautions to prevent virus infections on the District's equipment.
2. The downloading of any software or files without the approval of the Director of Network Services is strictly prohibited. Software is defined as but not limited to programs, games, browsers, and sound files, which can be downloaded from the Internet.
3. The illegal use of copyrighted software or files is prohibited. Copyright infringement occurs when you use and/or reproduce a work that is protected by a copyright.
4. The accessing of non-educational content games, chat rooms and recreational videos and music is strictly prohibited.
5. The District does not relinquish control over materials on the computer system or contained in files stored on the system.
6. The District reserves the right to suspend or terminate the computer systems access of users who have violated the AUP, and to delete or remove files found to be in violation of the AUP.
7. The District will report and cooperate fully with local, state, and federal authorities in any investigation concerning or related to any illegal activities conducted through the District computer network.

System Limits

1. Users shall access the system only for educational, professional or career development activities. This applies to discussion group mail lists, instant message services and

participation in Internet "chat room" conversations, and educational, safe and secure social networking platforms.
2. Users shall check e-mail frequently and delete messages promptly.
3. Users should compress graphics in all file types and delete large files.

Privacy Rights

1. Users shall respect the privacy of messages that they receive and refrain from reposting messages without the approval of the sender.
2. Users shall not publish private information about another individual.
3. A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the District's technology resources.

Adopted by State Superintendent: January 25, 2005
NJSBA Review/Update: November 2010
Readopted by State District Superintendent: December 21, 2010
Revised by State District Superintendent: March 27, 2012

Key Words:

Acceptable Use, Internet Safety, Social Networking, Cyberbullying, Blocking/Filtering Software, E-mail, Internet, Technology, Web Site, World Wide Web

Legal References:		
	N.J.S.A. 2A:35A-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 Districts contents; Annual report of commissioner's report on Improvement of basic skills
	N.J.S.A. 18A:7A-35	State District Superintendent of Schools
	N.J.S.A. 18A:7A-38	Power of Superintendent
	N.J.S.A. 18A: 36-35	School Internet Websites; disclosure of certain Student information prohibited
	N.J.S.A. 18A:36-35	School Internet Websites: disclosure of certain student information prohibited
	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
	47 U.S.C. 254(l)	Neighborhood Children's Internet Protection Act
	15 U.S.C. §§ 6501-6506	Children's Online Privacy Protection Act
	15 U.S.C. §§ 6551-6555	Promoting a Safe Internet for Children Act
	N.J. v. T.L O., 469 U.S. 325 (1985)	

TECHNOLOGY (continued)

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.

Manual for the Evaluation of Local School Districts (September 2002)

Possible Cross References:

*1111 District Publications
*3514 Equipment
*3570 District records and reports
*5114 Suspension and expulsion
*5124 Reporting to parent/guardians
*5131 Conduct/discipline
*5131.5 Vandalism/violence
*5142 Pupil Safety
*6144 Controversial issues
*6145.3 Publications

*Indicates policy is included in the Critical Policy Reference Manual