SECTION: 811

TITLE: Acceptable Use of the Computers, Network, Internet, Electronic Communications and Technical Services Policy

NESHAMINY SCHOOL DISTRICT

I. Purpose	The Neshaminy School District (NSD) provides employees, students, and guests (users) with access to the District's electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means. Guests include, but are not limited to, visitors, workshop attendees, volunteers, independent contractors, adult education staff, students, and board members. Computers, network, Internet, electronic communications and Technical Services (collectively "NIS") provide vast, diverse and unique resources. The Board of School Directors will provide access to the District's NIS systems for users if there is a specific District-related purpose to access information and research; to collaborate to facilitate learning and teaching; and to foster the educational purpose and mission of the District. For users, the District's NIS systems must be used for education-related purposes and performance of District job duties. Incidental personal use of school computers is permitted for employees so long as such use does not interfere with the employee's job duties and performance, with system operations, or with other system users. Personal use must comply with this policy and all other applicable District policies, procedures and rules contained in this policy, as well as Internet service provider ("ISP") terms, local, state and federal laws and must not damage the District's NIS systems. Students may only use the NIS systems for educational purposes. At the same time, personal technology devices brought onto the District's property, or to District events, or connected to the District's network, that the District reasonably believes contain District information or contain information that violates a District policy, or contain information/data that the District reasonably believes involves a criminal activity may be legally accessed to insure compliance with this policy, other District policies, and to comply with the law. Users may not use their personal electronic devices, including computers to connect to the District's intranet, Internet or any other NIS system unless approved by the Director of Technology and/or designee. The District intends to strictly protect its NIS systems against numerous outside and internal risks and vulnerabilities. Users are important and critical players in protecting these District assets and in lessening the risks that can destroy these important and

POLICY 811 (cont'd)

critical assets. Consequently, users are required to fully comply with this policy, and to immediately report any violations or suspicious activities to the Director of Technology and/or building lab aide for staff; and to teacher, guidance counselor, and/or building principal. Conduct otherwise will result in actions further described in Section VI – Guidelines – Consequences for Inappropriate, Unauthorized and Illegal Use, found in the last section of this policy, and provided in relevant District policies.

II. Definitions

Child Pornography – Under Federal law, any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:

a. the production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;
b. such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or
c. such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Under Pennsylvania law, any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of 18 years engaging in a prohibited sexual act or in the simulation of such act is prohibited.

Computer – Includes any District owned, leased or licensed or user owned personal hardware, software, or other technology used on District premises or at District events, or connected to the District network, containing District programs or District or student data (including images, files, and other information) attached or connected to, installed in, or otherwise used in connection with a computer. Computer includes, but is not limited to, District and users': desktop, notebook, PowerBook, tablet PC or laptop computers, printers, facsimile machine, cables, modems, and other peripherals; specialized electronic equipment used for students' special educational purposes; global Positioning System (GPS) equipment; personal digital assistants (PDAs); iPods, IPADS, MP3 players; cell phones, with or without Internet access and/or recording and/or camera/video and other capabilities and configurations, telephones, mobile phones, or wireless devices, two-way radios/telephones; beepers; paging devices, laser pointers and attachments, and any other such technology developed.

Electronic Communications Systems – Any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used

POLICY 811 (cont'd)

for such purposes. Further, an electronic communications system means any wire, radio, electromagnetic, photo-optical or photo-electronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications. Examples include, without limitation, the Internet, intranet, electronic mail services, GPS, PDAs, facsimile machines, cell phones with or without Internet access and/or electronic mail and/or electronic mail and/or recording devices, cameras/video, and other capabilities or configurations.

Educational Purpose – Includes use of the NIS systems for classroom activities, professional or career development, and to support the District's curriculum, policy and mission statement.

Harmful to Minors – Under Federal law, any picture, image, graphic image file or other visual depictions that:

a. taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion;
b. depicts, describes, or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and
c. taken as a whole, lacks serious literary, artistic, political, educational or scientific value as to minors.

Under Pennsylvania law, any description or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

a. predominantly appeals to the prurient, shameful, or morbid interest of minors; and
b. is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and
c. taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors.

Incidental Personal Use – Incidental personal use of school computers is permitted for employees so long as such use does not interfere with the employee's job duties and performance, with system operations, or with other system users. Personal use must comply with this policy and all other applicable District procedures, rules contained in this policy, school rules and directives, as well as ISP terms, local, state and federal laws and must not damage the District's NIS systems.

Minor – For purposes of compliance with the Children's Internet Protection Act ("CIPA"), an individual who has not yet attained the age of seventeen. For other purposes, minor shall mean the age of minority as defined in the relevant law.

POLICY 811 (cont'd)

Obscene – Under Federal law, analysis of the material meets the following elements:

a. whether the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;
b. whether the work depicts or describes, in a patently offensive way, sexual conduct specifically designed by the applicable state or federal law to be obscene; and
c. whether the work taken as a whole lacks serious literary, artistic, political, educational, or scientific value.

Under Pennsylvania law, analysis of the material meets the following elements:

a. the average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;
b. the subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and
c. the subject matter, taken as a whole lacks serious literary, artistic, political, educational or scientific value.

Sexual Act and Sexual Contact – As defined at 18 U.S.C. § 2246(3), 18 Pa.C.S.A. § 5903.

Technology Protection Measure(s) – A specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.

Visual Depictions – Undeveloped film and videotape and data stored on computer disk or by electronic means which is capable of conversion into a visual image but does not include mere words.

III. Authority

Access to the District's NIS systems through school resources is a privilege, not a right. These, as well as the user accounts and information, are the property of the District, which reserves the right to deny access to prevent further unauthorized, inappropriate or illegal activity, and may revoke those privileges and/or administer appropriate disciplinary action. The District will cooperate to the extent legally required with ISP, local, state and federal officials in any investigation concerning or related to the misuse of the NIS systems.

It is often necessary to access user accounts, including but not limited to email boxes, network folders, and hard drives on the District-assigned laptop or desktop, in order to perform routine maintenance and security tasks; system administrators have the right to access by interception, and the stored communication of user accounts for any reason in order to uphold this policy and to maintain the system. Users have no privacy expectation in the contents of their personal files or any of their use of the District's NIS systems. The District reserves the right to monitor, track, log and access

POLICY 811 (cont'd)

NIS systems use and to monitor and allocate fileserver space.

The District reserves the right to restrict access to any Internet sites or functions it may deem inappropriate through general policy, software blocking or online server blocking. Specifically, the District operates and enforces technology protection measure(s) that block or filter online activities of minors on its computers used and accessible to adults and students so as to filter or block inappropriate matter on the Internet. Inappropriate matter includes, but is not limited to, visual, graphic, text and any other form or obscene, sexually explicit, child pornographic, or other material that is harmful to minors, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying, terroristic, and advocates the destruction of property. Measures designed to restrict adults' and minors' access to material harmful to minors may be disabled to enable an adult or student to access bona fide research, not within the prohibitions of this policy, or for another lawful purpose. No person may have access to material that is illegal under federal or state law. Expedited review and resolution of a claim that the policy is denying a student or adult to access material will be enforced by an administrator, supervisor, or their designee upon the receipt of written consent from a parent or guardian of a student, and upon the written request from an adult.

The District has the right, but not the duty, to monitor, track, log, access and/or report all aspects of its computer information, technology and related systems of all users and of any user's personal computers, network, Internet, electronic communication systems, and media that they bring onto District property, or to District events, that were connected to the District network, which contained District programs or District or student data (including images, files, and other information), all pursuant to the law, in order to insure compliance with this policy and other District policies, to protect the District's resources, and to comply with the law.

The District reserves the right to restrict or limit usage of lower priority NIS systems and computer uses when network and computing requirements exceed available capacity according to the following priorities:

a. Highest – uses that directly supports the education of students.
b. Medium – uses that indirectly benefit the education of the students.
c. Lowest – uses that include reasonable and limited educationally-related interpersonal communications.
d. Forbidden – all activities in violation of this policy.

The District additionally reserves the right to:

a. Determine which NIS systems' services will be provided through District resources. The Director of Elementary and Secondary Education, the

POLICY 811 (cont'd)

Director of Technology, and the Director of Curriculum, Assessment, and Instruction will jointly determine this.

b. Determine the types of files that may be stored on District file servers and computers. The Director of Technology will determine this.

c. View and monitor network traffic, file server space, processor, and system utilization, and all applications provided through the network and communications systems, including e-mail and other electronic communications. The Director of Technology will perform this.

d. Remove excess e-mail or files taking up an inordinate amount of fileserver disk space after a reasonable time. The Director of Technology will perform this as authorized by the building principal or supervisor.

e. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable District policies occur or state or federal law is violated, including, but not limited to, those governing network use, copyright, security, privacy, employment, data breaches, and destruction of District resources and equipment. The Director of Technology will perform this, with authorization from the appropriate Business Office Administrator, building principal, or employee supervisor.

IV. Responsibility

Due to the nature of the Internet as a global network connecting thousands of computers around the world, inappropriate materials, including those which may be defamatory, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), inaccurate, obscene, sexually explicit, lewd, vulgar, rude, harassing, violent, inflammatory, threatening, terroristic, hateful, bullying, profane, pornographic, offensive, or illegal, can be assessed through the network and electronic communications systems. Because of the nature of the technology that allows the Internet to operate, the District cannot completely block access to these resources. Accessing these and similar types of resources may be considered an unacceptable use of school resources and will result in actions explained further under **Consequences for Inappropriate, Unauthorized and Illegal Use**, found in the last section of this policy and as provided in relevant District policies.

Users must be capable and able to use the District's NIS systems, and software relevant to their responsibilities. In addition, users must follow the "best practices" guidelines developed by the Director of Technology, practice proper etiquette, District ethics, and agree to the requirements of this policy.

V. Delegation of Responsibility

The Director of Technology and/or designee will serve as the coordinator to oversee the District's NIS systems and will work with other regional or state organizations as necessary, to educate users, approve activities, provide leadership for proper training for all users in the use of the NIS systems and the requirements of

POLICY 811 (cont'd)

this policy, establish a system to insure adequate supervision of the NIS systems, maintain executed user agreements, and interpret and enforce this policy.

The Director of Curriculum and Instruction or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including but not limited to:

a. Interaction with other individuals on social networking web sites and in chat rooms.
b. Cyberbullying awareness and response.

The Director of Technology and/or designee will establish a process for setting-up individual and class accounts, develop "best practices" guidelines for users to manage their e-mail boxes and network folders, set quotas for disk usage on the system, establish a Policy and Schedule for the retention and destruction of District electronically stored information, and establish the District virus protection process.

Unless otherwise denied for cause, student access to the NIS systems resources shall be through supervision by the professional staff. Administrators, teachers and staff have the responsibility to work together to help students develop the skills and judgment required to make effective and appropriate use of the resources. All users have the responsibility to respect the rights of all other users within the District and District NIS systems, and to abide by the rules established by the District, its ISP, local, state and federal laws.

VI. Guidelines

Access to the NIS Systems

a. NIS system user accounts will be used only by authorized owners of the accounts for authorized purposes.
b. An account will be made available according to a procedure developed by appropriate District authorities and performed by the Director of Technology, or designee.
c. Types of Services include, but are not limited to:
    1) World Wide Web. District employees, students, and guests will have access to the Web through the District's NIS systems as needed.
    2) E-Mail. District employees may be assigned individual e-mail accounts for work related use, as needed. Students may be assigned individual e-mail accounts, as necessary, by the Director of Technology and/or designee, and at the recommendation of the teacher who will also supervise the students' use of the e-mail service.
    3) Guest Accounts. Guests may receive an individual account with the approval of the Director of Technology and/or designee if there is a specific District-related purpose requiring such access. Use of the NIS systems by a guest must be specifically limited to the District-related purpose and comply with this policy and all other District policies,

POLICY 811 (cont'd)

procedures and rules, as well as Internet Service Provider ("ISP") terms, local, state and federal laws and may not damage the District's NIS systems. An agreement between the District and a Guest, and a parental signature will be required if the Guest is a minor.

4) Web 2.0 Second Generation Web-based Services. Certain District authorized Second Generation Web-based services, such as social networking sites, wikis, podcasts, RSS feeds, social software, folksonomies and collaboration tools that emphasize online educational collaboration and sharing among users may be permitted by the District, however, such use must be approved by the Director of Curriculum, Assessment and Instruction, or designee, followed by training authorized by the District. Users must comply with this policy, as well as any other relevant policy, regulations or rules during such use.

Comm v. Cass, 551 Pa. 25 (1998); *New Jersey v. T.L.O.*, 469 U.S. 325 (1985); *O'Connor v. Ortega*, 480 U.S. 709 (1987)

d. Access to all data on, taken from, or compiled using District computers is subject to inspection and discipline. Users have no right to expect that District information placed on users' personal computers, networks, Internet, and electronic communications systems is beyond the access of the District. The District reserves the right to access users' personal technology devices brought onto the District's property, or to District events, or connected to the District's network, when the District reasonably believes they contain District information or contain information that violates a District Policy, or contains information/data that the District reasonably believes involves a criminal activity.

Parental Notification and Responsibility

The District will keep this policy posted on its website. This policy contains restrictions on accessing inappropriate material. There is a wide range of material available on the Internet, some of which may not be fitting with the particular values of the families of the students. It is not practically possible for the District to monitor and enforce a wide range of social values in student use of the Internet. Further, the District recognizes that parents bear primary responsibility for transmitting their particular set of family values to their children. The District will encourage parents to specify to their child(ren) what material is and is not acceptable for their child(ren) to access through the District's NIS system. Parents are responsible for monitoring their children's use of the District's NIS system when they are accessing the systems from outside of the District.

School District Limitation of Liability

The District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the District's NIS systems will be error-free or without defect. The District does not warrant the effectiveness of Internet filtering. The electronic information available to users does not imply

POLICY 811 (cont'd)

endorsement of the content by the District, nor is the District responsible for the accuracy or quality of the information obtained through or stored on the NIS systems. The District shall not be responsible for any damage users may suffer, including but not limited to, information that may be lost, damaged, delayed, misdelivered, or unavailable when using the computers, network and electronic communications systems. The District shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The District shall not be responsible for any unauthorized financial obligations, charges or fees resulting from access to the District's NIS systems. In no event shall the District be liable to the user for any damages whether direct, indirect, special or consequential, arising out of the use of the NIS systems.

Prohibitions

The use of the District's NIS systems for illegal, inappropriate, unacceptable, or unethical purposes by users is prohibited. Such activities engaged in by users are strictly prohibited and illustrated below. The District reserves the right to determine if any activity not appearing in the list below constitutes an acceptable or unacceptable use of the NIS systems.

These prohibitions are in effect any time District resources are accessed whether on District property, when using mobile computing equipment, telecommunication facilities in unprotected areas or environments, directly from home, or indirectly through another ISP, and if relevant, when an employee or student uses their own equipment.

Students are prohibited from visually possessing and using their personal computers on District premises and property (including but not limited to buses and other vehicles), at District events, or through connection to the District NIS systems, unless expressed permission has been granted by a teacher or administrator, who will then assume the responsibility to supervise the student in its use, or, unless an IEP team determines otherwise, in which case, an employee will supervise the student in its use. Students at the high school level are permitted to use their cell phones during the change of classes. Thus, in general, students are prohibited from using cell phones, with or without Internet access and/or recording and/or camera/video and other capabilities and configurations.

Cameras, and the like, may not be used to take images of others, transfer them, or place them on websites without the consent of the building principal. Students who are performing volunteer fire company, ambulance or rescue squad functions, or need such a computer due to their medical condition, or the medical condition of a member of their family, with notice and the approval of the school administrator may qualify for an exemption of this prohibition.

SC § 3-1317.1(b)

a. General Prohibitions

Users are prohibited from using District NIS systems to:

- Communicate about non-work or non-school related communications using District-assigned e-mail accounts.

POLICY 811 (cont'd)

- District employees may be allowed to access their personal ISP e-mail accounts through the Internet, provided it does not interfere with their job responsibilities and that it does not interfere with other employee job-related use of computer and network resources.
- Students may be allowed to access their personal ISP e-mail accounts through the Internet, provided it is not done on class time and that it does not deny other students of computer and network resources.
- Examples of personal ISP accounts are AOL, Comcast, Verizon, Hotmail, Yahoo and Gmail.

- Send, receive, view, download, access or transmit material that is harmful to minors, indecent, obscene, pornographic, child pornographic, terroristic, or advocates the destruction of property.
- Send, receive, view, download, access or transmit inappropriate matter and material likely to be offensive or objectionable to recipients including, but not limited to, that which may be defamatory, inaccurate, obscene, sexually explicit, lewd, hateful, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, marital status, age, sexual orientation, political beliefs, receipt of financial aid or disability), violent, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic and/or illegal.
- Bully or cyberbully any staff member or student while on school property (or away from school grounds if the misconduct directly affects the health and safety of students or staff as well as the good order, efficient management and welfare of the District). Cyberbulling includes, but is not limited to the following misuses of technology: harassing, teasing, intimidating, threatening or terrorizing a staff member or student of the District.
- Access or transmit gambling, pools for money, including but not limited to, basketball and football, or any other betting or games of chance.
- Participate in discussion or news groups that cover inappropriate and/or objectionable topics or materials, including those that conform to the definition of inappropriate matter in this policy.
- Send terroristic threats, hateful mail, harassing communications, discriminatory remarks, and offensive or inflammatory communications.
- Participate in unauthorized Internet Relay Chats, instant messaging communications (on-line; real-time conversations) that are not for school-related purposes or required for employees to perform their job duties.

NSD Board Policy 553

11 P.S. § 311, et seq.

18 Pa.C.S.A. § 2706, § 2709, § 27009.1

POLICY 811 (cont'd)

- Facilitate any illegal activity.
- Communicate through District e-mail for non-educational purposes or activities. The use of e-mail to mass mail non-educational or non-work related information is expressly prohibited (for example, the use of the "everyone distribution list," building level distribution lists, or other e-mail distribution lists to offer personal items for sale is prohibited.
- Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable District policies); conduct unauthorized fund raising or advertising on behalf of the District and non-school District organizations; resale of District computer resources to individuals or organizations; or use the District's name in any unauthorized manner that would reflect negatively on the District, its employees, or students. Commercial purposes is defined as offering or providing goods or services or purchasing goods or services for personal use. District acquisition policies will be followed for District purchase of goods or supplies through the District system.
- Engage in political lobbying.
- Install, distribute, reproduce or use copyrighted software on District computers, or copy District software to unauthorized computer systems, intentionally infringing upon the intellectual property rights of others or violating a copyright.
- Install computer hardware, peripheral devices, network hardware or system hardware. The authority to install hardware or devices on District computers is restricted to the Director of Technology or designee.
- Encrypt messages using encryption software that is not authorized by the District from any access point on District equipment or District property. Users must use District approved encryption to to protect the confidentiality of sensitive or critical information in the District's approved manner.
- Access, interfere, possess, or distribute confidential or private information without permission of the District's administration. An example includes accessing other students' accounts, including, but not limited to, obtaining their personal demographics, grades, library accounts and lunch account. Reference the Pennsylvania Department of Education Student Access and Use Policy.

POLICY 811 (cont'd)

- Violate the privacy or security of electronic information.
- Send any District information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the District's business, or educational interest. Reference the Pennsylvania Department of Education Student Access and Use Policy.
- Send unsolicited commercial electronic mail messages, also known as spam.
- Post personal or professional web pages without administrative approval.
- Post anonymous messages.
- Use the name of the "Neshaminy School District" in any form in Web "blogs," on District Internet pages or websites not owned or related to the District, or in forums/discussion boards to express or imply the position of the Neshaminy School District without the expressed, written permission of the Superintendent. When such permission is granted, the posting must state that the statement does not represent the position of the District.
- Users are not permitted to have blogs without the review and approval of the Director of Curriculum, Assessment & Instruction and their building principal. All bloggers must follow the rules provided in this policy and other applicable policies, regulations and rules provided in this policy and other applicable policies, regulations and rules of the District.
- Bypass or attempt to bypass Internet filtering software by any method including, but not limited to, the use of anonymizers/ proxies or any websites that mask the content the user is accessing or attempting to access.
- Advocate illegal drug use, whether expressly or through a latent pro-drug message. This does not include a restriction on political or social commentary on issues, such as the wisdom of the war on drugs or medicinal use.
- Attempt to and/or obtain personal information under false pretenses with the intent to defraud another person, including, but not limited to, spoofing and phishing.

b. Access and Security Prohibitions

Users must immediately notify the Director of Technology and/or designee if they have identified a possible security problem.

All users must read, understand, and comply with this policy that includes network, Internet usage, electronic communications, telecommunications,

POLICY 811 (cont'd)

nondisclosure and physical and information security policies. Staff users must provide a signed acknowledgement form. Staff users with access to student data must read, understand and sign the Pennsylvania Department of Education Student Access and Use Policy's Student Data Non-disclosure Agreement. The following activities related to access to the District's NIS systems, and information are prohibited:

- Misrepresentation (including forgery) of the identity of a sender or source of communication, including, but not limited to, spoofing and phishing.
- Acquiring or attempting to acquire passwords of another. Users will be held responsible for the result of any misuse of users' names or passwords while the users' systems access were left unattended and accessible to others, whether intentional or through negligence.
- Using or attempting to use computer accounts of others, these actions are illegal, even with consent, or if only for the purpose of "browsing."

18 Pa.C.S.A. § 7611, et seq.

- Using District resources to engage in any illegal act, which may threaten the health, safety or welfare of any person or persons, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal activity, or being involved in a terroristic threat against any person or property.
- Disabling or circumventing any District security, program or device, for example, but not limited to, anti-spyware, anti-spam software, and virus protection software or procedures.
- Transmitting electronic communications anonymously or under an alias unless authorized by the District.
- Users must protect and secure all electronic resources and information, data and records of the District from theft, and inadvertent disclosure to unauthorized individuals or entities when they are under the supervision and control of the District, and when they are not under the supervision or control of the District, for example, but not limited to, working at home, on vacation, or elsewhere. If any user becomes aware of the release District information, data or records, the release must be immediately reported to the Director of Elementary & Secondary Education. At the direction of the Director of Elementary & Secondary Education, the Director of Technology will analyze the breech to determine its scope. Reference the Pennsylvania Department of Education Student Access and Use Policy for further information.

c. Operational Prohibitions

The following operational activities and behaviors are prohibited:

POLICY 811 (cont'd)

- Interference with or disruption of the NIS systems, network accounts, services or equipment of others, including, but not limited to, the propagation of computer "worms" and "viruses," Trojan Horse and trapdoor program code, the sending of electronic chain mail, distasteful jokes, and the inappropriate sending of "broadcast" messages to large numbers of individuals or hosts.
- User may not hack or crack the network or others' computers, whether by parasiteware or spyware designed to steal information, or viruses and worms or other hardware or software designed to damage the NIS systems, or any component of the network, or strip or harvest information, or completely take over a person's computer, or to "look around."
- Altering or attempting to alter files, system security software or the systems without authorization.
- Unauthorized scanning of the NIS systems for security vulnerabilities.
- Attempting to alter any District computing or networking components (including, but not limited to fileservers, bridges, routers, switches, wireless access point, or hubs) without authorization or beyond one's level of authorization.
- Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension of retransmission of any computer, electronic communications systems, or network services, whether wired, wireless, cable, or by other means.
- Connecting unauthorized hardware and devices to the NIS systems.
- Loading, downloading, or use of unauthorized games, programs, files, or other electronic media, including, but not limited to, downloading music files, movies and video clips.
- Intentionally damaging or destroying the integrity of the District's electronic information.
- Intentionally destroying the District's computer hardware or software.
- Intentionally disrupting the use of the NIS systems.
- Damaging the District's NIS systems, networking equipment through the users' negligence or deliberate act.
- Failing to comply with requests from appropriate teachers or District administrators to discontinue activities that threaten the operation or integrity of the NIS systems.

d. Conducting Union Business

- The recognized bargaining unit shall have the right to use school equipment as per the contract agreement.

POLICY 811 (cont'd)

Content Guidelines

Information electronically published on the District's NIS systems shall be subject to the following guidelines:

a. Published documents including but not limited to audio and video clips or conferences, may not include a student's phone number, street address, or box number, name (other than first name) or the names of other family members without parental consent.

b. Documents, web pages, electronic communications, or videoconferences may not include personally identifiable information that indicates the physical location of a student at a given time without parental consent.

c.. Documents, web pages, electronic communications, or videoconferences may not contain objectionable materials or point directly or indirectly to objectionable materials.

d. Documents, web pages and electronic communications, must conform to all District policies and guidelines, including the copyright policy.

e. Documents to be published on the Internet must be reviewed, edited and approved by the Director of Curriculum, Assessment and Instruction before publication.

Comm v. Cass, **551 Pa. 25 (1998);** *New Jersey v. T.L.O.,* **469 U.S. 325 (1985);** *O'Connor v. Ortega,* **480 U.S. 709 (1987);**

Title 17, U.S.C.

Termination

The District reserves the right to terminate the account privileges of any user at any time. The District will endeavor to provide notice to the user of such termination.

System Monitoring

a. Users' violations of this policy, any other District policy, or the law may be discovered by routine maintenance and monitoring of the District system, or pursuant to any legal means.

b. The District reserves the right to monitor, track, log and access any electronic communications, including but not limited to, application system access, network folders, Internet access and e-mails at any time for any reason. Users should not have any expectation of privacy in their use of the District's NIS systems, and other District technology, even if they use the NIS system for personal reasons. Further, the District reserves the right, but not the obligation, to legally access any personal technology device of students and employees brought onto the District's property or to District events, or connected to the District network, containing District programs or District or student data (including images, files, and other information) to insure compliance with this policy and other District policies, to protect the District's resources, to obtain information/data that the District reasonably believes involves criminal activity.

c. Everything that users place in their personal files should be written as if a third party will review it.

POLICY 811 (cont'd)

Copyright Infringement and Plagiarism

a. Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the District resources. Users will make a standard practice of requesting permission from the holder of the work complying with license agreements. Employees will instruct users to respect copyrights, request permission when appropriate, and comply with license agreements. Employees will respect and comply as well.

b. Violations of copyright law can be a felony and the law allows a court to hold individuals personally responsible for infringing the law. The District does not permit illegal acts pertaining to the copyright law. Therefore, any user violating the copyright law does so at their own risk and assumes all liability.

c. Violations of copyright law include, but are not limited to, the making of unauthorized copies of any copyrighted material (such as commercial software, text, graphic images, audio and video recording), distributing copyrighted materials over computer networks, and deep-linking and framing into the content of others' web sites. Further, the illegal installation of copyrighted software or files for use on the District's computers are expressly prohibited. This includes all forms of licensed software – shrink-wrap, click wrap, browse wrap, and electronic software downloaded from the Internet.

d. District guidelines on plagiarism will govern use of material accessed through the District's NIS systems. Users will not plagiarize works that they find. Teachers will instruct students in appropriate research and citation practices.

Selection of Material

a. District policies on the selection of materials will govern use of the District's NIS systems must be approved by the Director of Curriculum, Assessment and Instruction, with the appropriateness of operability approved by the Director of Technology.

b. When using the Internet for class activities, teachers will select material that is appropriate in light of the age of the students and that is relevant to the course objectives. Teachers will preview the materials and web sites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the web site. Teachers will provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the critical thinking skills necessary to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.

POLICY 811 (cont'd)

School District Website

The District will establish and maintain a website and will develop and modify its web pages that will present information about the District under the direction of the Director of Curriculum, Assessment and Instruction and/or designee.

Safety & Privacy

a. To the extent legally required, users of the District's NIS systems will be protected from harassment or commercially unsolicited electronic communication. Any user who receives threatening or unwelcome communications must immediately send or take them to the Director of Technology and/or designee.

b. Users will not post personal contact information about themselves or other people on the NIS systems. The user may not steal another's identity in any way, may not use spyware, cookies, or use District or personal technology or resources in any way to invade one's privacy. Additionally, the user may not disclose, use or disseminate confidential and personal information about students or employees (examples include, but are not limited to, using a PDA, iPod, MP3; cell phone with camera/ video and Internet access to take pictures of anything, including but not limited to, persons, places, and documents relevant to the District, saving, storing and sending the image with or without text or disclosing them by any means, including but not limited to, print and electronic matter; revealing student grades, social security numbers, home addresses, telephone numbers, school addresses, work addresses, credit card numbers, health and financial information, evaluations, psychological reports, educational records, reports, and resumes or other information relevant to seeking employment at the District unless legitimately authorized to do so). Reference the Pennsylvania Department of Education Student Access and Use Policy for further information.

c. Student users will agree not to meet with someone they have met online unless they have parental consent.

Children's Internet Protection Act
47 U.S.C. § 254
34 C.F.R. 54.520

Child Internet Protection Act
24 P.S. § 4601 et seq.

d. Internet safety measures shall effectively address the following:

- Control of access by minors to inappropriate matter on the Internet and World Wide Web.
- Safety and security of minors when using electronic mail, chat rooms, and other forms of direct communications.
- Prevention of unauthorized access by minors, including "hacking" and other unlawful activities.
- Unauthorized disclosure, use, and dissemination of personal information regarding minors.
- Restrict of minors access to materials harmful to them.

Consequences for Inappropriate, Unauthorized and Illegal Use

a. General rules for behavior, ethics, and communications apply when using the NIS systems and information, in addition to the stipulations of this

POLICY 811 (cont'd

policy. Users must be aware that violations of this policy or other policies, or for unlawful use of the NIS systems may result in loss of NIS access and a variety of other disciplinary actions, including but not limited to, warnings, usage restrictions, loss of privileges, position reassignment, oral or written reprimands, suspensions (with or without pay for employees), dismissal, expulsions, and/or legal proceedings on a case-by-case basis. This policy incorporates all other relevant District policies, such as, but not limited to, the student and professional employee discipline policies, copyright policy, property policy, curriculum policies, terroristic threat policy, and harassment policies.

b. The user is responsible for damages to the network, equipment, electronic communications systems, and software resulting from deliberate and willful acts. The user will also be responsible for incidental or unintended damage resulting from willful or deliberate violations of this policy.

c. Violations as described in this policy may be reported to the District, appropriate legal authorities, whether the ISP, local, state, or federal law enforcement. The District will cooperate to the extent legally required, with authorities in all such investigations.

d. Vandalism will result in cancellation of access to the District's NIS systems and resources and is subject to discipline.

Approved: June 2012

Rev/App: February 2013

JR/KC/sab

Neshaminy School District
Technology Use Guidelines for Staff

Supplement to Policy 811 – Acceptable Use of the Computers, Network, Internet, Electronic Communications and Technical Services

OVERVIEW

- The Neshaminy School District (NSD) intends to strictly protect the system against outside and internal risks and vulnerabilities. The NSD provides staff with access to the District's network, which includes Internet access, whether wired or wireless, or by any other means. The information in this guideline aligns with Policy 811, Acceptable Use of the Computers, Network, Internet, Electronic Communications and Technical Services which goes into much further detail on the use of the District Network resource. [This and all other policies are accessible on the Neshaminy School District website.]

Network and Internet Responsibility

- Network accounts will be used only by the authorized owner of the account for its authorized purpose. All communication and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.
- NSD reserves the right to access user accounts, including but not limited to email boxes, network folders, and hard drives on District-assigned laptops or desktop computers, in order to perform routine maintenance and security tasks.
- Access to all data on, taken from or compiled using District computers is subject to inspection and discipline.
- Staff may not:
    - post personal communications in public forum without the original author's prior consent
    - install, distribute, reproduce or use copyrighted software on District computers, or copy District software to unauthorized computer systems
    - install computer hardware, peripheral devices, network hardware or system hardware
    - access, interfere, posses, or distribute confidential or private information
    - post anonymous messages
    - bypass or attempt to bypass Internet filtering software by any methods including, but not limited to, the use of proxies
    - acquire or attempt to acquire passwords of another or the misuse of another user's name and password
    - use a computer that has been logged-in under another user's name
    - disable or circumvent any District security, program or device
    - scan the NSD system for security vulnerabilities
    - load, download or use unauthorized games, programs, files or other electronic media, including, but not limited to, downloading music files, movies and video clips
    - use the network to disrupt the work of other users
    - use the network to access obscene or pornographic material or inappropriate language or profanity on the network
    - use the network for commercial or for profit purposes, product advertisement or political lobbying

Sanction and Violations

The network user shall be responsible for damages to the equipment, systems and software or other resources resulting from deliberate or willful acts. These may be reported to law enforcement.
Violations may result in a limited or immediate total loss of right to the District's technology.

Additional disciplinary action may be determined at the District level in line with the Employee Handbook and the District's Code of Conduct.

Technology Usage Agreement

Disclaimer

The NSD makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the staff may suffer while on this system. These damages may include, but are not limited to: loss of data as a result of delays, non-deliveries, mis-deliveries, or service interruptions caused by the system or by staff error or omission. Use of any information obtained via the information system is at the staff's own risk.

Employee

I have read the School District's "Technology Use Guidelines for Staff" which reflects Policy 811 – Acceptable Use of the Computers, Network, Internet, Electronic Communications and Technical Services. A copy is available at https://neshaminy.org

I also understand that this policy will be reviewed yearly and additional rules, regulations, and/or guidelines may be added from time to time and that they will become a part of this agreement.

I hereby release the District, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my use of, or inability to use, the electronic network. This includes, but is not limited to, claims that may arise from the unauthorized use of the network components. I understand that inappropriate or illegal use of technology could result in civil or criminal lawsuits.

Employee Signature_____ Date _____

Employee Name (please print) _____

Neshaminy School District

Technology Use Guidelines for Students

Supplement to Policy 811 - Acceptable Use of the Computers, Network, Internet, Electronic Communications and Technical Services

OVERVIEW

- The Neshaminy School District (NSD) network is for educational purposes. The District intends to strictly protect the NSD system against outside and internal risks and vulnerabilities. The NSD provides student with access to the District's network, which includes Internet access, whether wired or wireless, or by any other means. The information in this guideline aligns with Policy 811 – Acceptable Use of the Computers, Network, Internet, Electronic Communications and Technical Services, which goes into much further detail on the use of the District Network resource. [This and all other policies are accessible on the Neshaminy School District website.]

Network and Internet Responsibility

- Students may not use their personal electronic device (PED) during the school day. This can include, but is not limited to, laptops, notebooks, electronic readers (such as Kindles, Nook, etc.), iPads, Tablets, iPods, cell phones, etc [unless authorized by a teacher].
- NSD reserves the right to access user accounts, including but not limited to email boxes, network folders, and hard drives on District-assigned laptops or desktop computers, in order to perform routine maintenance and security tasks.
- Access to all data on, taken from or compiled using District computers is subject to inspection and discipline.
- Approved Web 2.0 tools, such as wikis, podcasts and collaboration tools that emphasize online education collaboration and sharing among users may be permitted by the District.
- Students may not use the school Internet for the purpose of social networking, including sites such as MySpace, Facebook, or to chat or access unauthorized chat rooms.
- Students may be allowed to access their personal ISP e-mail account through the Internet, provided it is not done on class time and provided that it does not deny other students of computer and network resources.
- Students may not:
    - send, receive, view, download, access or transmit material that is not educational, or not approved by a teacher
    - participate in discussion or news groups
    - send terroristic threats
    - install, distribute, reproduce or use copyrighted software on District computers, or copy District software to unauthorized computer systems
    - install computer hardware, peripheral devices, network hardware or system hardware
    - access, interfere, possess, or distribute confidential or private information
    - post anonymous messages
    - bypass or attempt to bypass Internet filtering software by any methods including, but not limited to, the use of proxies
    - cyber bully another individual or entity
    - acquire or attempt to acquire passwords of another, or the misuse of another user's name and password
    - disable or circumvent any District security, program or device
    - scan the NSD system for security vulnerabilities
    - load, download or use unauthorized games, programs, files or other electronic media, including, but not limited to, downloading music files, movies and video clips

Sanctions and Violations

Any violation will be considered with respect to the circumstances within which it occurred. The following will apply:

1. Violations may result in a limited or immediate total loss of right to the Districts technology.
2. Additional disciplinary action may be determined at the building level in line with the Student Handbook and the District's Code of Conduct. This may include suspension and recommendations for expulsion.
3. Violation involving threats, theft or damage to equipment or other resources may be reported to law enforcement.

Technology Usage Agreement

Disclaimer

The NSD makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the student may suffer while on this system. These damages may include, but are not limited to: loss of data as a result of delays, non-deliveries,
mis-deliveries, or service interruptions caused by the system or by student error or omission. Use of any information obtained via the information system is at the student's own risk.

Parent/Guardian

I have read the School District's "Technology Use Guidelines for Students", which reflects Policy 811 – Acceptable Use of the Computers, Network, Internet, Electronic Communications and Technical Services. A copy is available at https://neshaminy.org

I also understand that this policy will be reviewed yearly and additional rules, regulations, and/or guidelines may be added from time to time and that they will become a part of this agreement.

I understand that my child may receive disciplinary consequences for inappropriate or unacceptable use of technology.

I understand that the District does everything possible to filter and restrict access to inappropriate material and I understand that it is impossible for the District to filter or restrict access to all inappropriate materials. I will not hold the District responsible for inappropriate or unacceptable materials my child may acquire while using the District's technology. I understand that inappropriate or illegal use of technology could result in civil or criminal lawsuits.

I hereby release the District, its personnel, and any institutions with which it is affiliated, from any and all claims and damages of any nature arising from my child's use of, or inability to use, the electronic network. This includes, but is not limited to, claims that may arise from the unauthorized use of the network components.

I give permission for my child to access all components of the District's technology which includes Internet access, computer services, videoconferencing, computer equipment and related equipment for educational purposes.

Parent/Guardian Signature_____ Date _____

Parent/Guardian Name (please print) _____

Student

I have read the School District's "Technology Use Guidelines for Students", which reflects Policy 811 – Acceptable Use of the Computers, Network, Internet, Electronic Communications and Technical Services. A copy is available at https://neshaminy.org

I agree to follow the rules contained in these guidelines.

I also understand that this policy will be reviewed yearly and additional rules, regulations, and/or guidelines may be added from time to time and that they will become a part of this agreement.

I understand that I may receive disciplinary consequences for inappropriate or unacceptable use of technology.

Student Signature _____ Date _____
(Secondary students only)

Student Name (please print) _____