Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Computers, Network, Internet, Electronic Communications and Technical Services
Code	815
Status	Active
Adopted	March 26, 2019

Purpose

The district provides employees, students, and other authorized users (guests) with access to the district's electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means. For purposes of this policy, **guests** include but are not limited to visitors, workshop attendees, volunteers, independent contractors, adult education staff and students, and Board members.

Computers, network, Internet, electronic communications and technical services (collectively known as NIS systems) provide vast, diverse and unique resources. The Board shall 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 as defined in this policy. 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.

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 district assets and in lessening the risks that can destroy these important and 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 or designee. Violations of this policy shall result in actions further described in this policy and provided in relevant district policies.

Definitions

The term child pornography is defined under both federal and state law.

Child pornography - under federal law, is 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:[1]

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

2. 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

3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Child pornography - under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.[2]

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: 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.

Educational purpose - includes use of the NIS systems for classroom activities, professional or career development, and to support the district's curriculum, policies and mission statement.

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 for such purposes. Further, an **electronic communications system** means any wire, radio, electromagnetic, photooptical or photoelectronic 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, but are not limited to: the Internet, intranet, electronic mail services, GPS, PDAs, facsimile machines, cell phones with or without Internet access and/or electronic mail and/or recording devices, cameras/video, and other capabilities or configurations.

The term harmful to minors is defined under both federal and state law.

Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depictions that:[3][4]

1. Taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex or excretion;

2. 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 contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals; and

3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.

Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:[5]

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;

2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and

3. Taken as a whole, lacks serious literary, artistic, political, educational or scientific value for minors.

The term **hacking** refers to the act of gaining unauthorized entry or attempting to gain unauthorized access to Neshaminy's computer network, servers, computers, system and/or data files, or the use of

Neshaminy School District resources, for the purpose of:

1. Determining the data structure and security restrictions of the computer system.

2. Making unauthorized changes in the data structure and security restrictions of the computer system.

3. Making unauthorized use of services provided by the computer system for purposes of sharing information regarding all of the above with other unauthorized users.

Incidental personal use - incidental personal use of 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 policies, procedures and rules, 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 (17). For other purposes, minor shall mean the age of minority as defined in the relevant law.[3][4]

Obscene - any material or performance if:[5]

1. The average person, applying contemporary community standards, would find that the subject matter, taken as a whole, appeals to the prurient interest;

2. The subject matter depicts or describes, in a patently offensive way, sexual conduct described in the law to be obscene; and

3. 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 and 18 Pa. C.S.A. §5903.[5][6]

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.[4]

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

Authority

Access to the district's NIS systems through school resources is a privilege, not a right. NIS systems, 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.[7][8][9]

It is often necessary to access user accounts, including but not limited to email, network folders and hard drives on a district-assigned laptop or desktop, in order to perform routine maintenance and security tasks. System administrators have the right to access the stored communication of user accounts in order to uphold this policy and to maintain the system. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the district's NIS systems, including personal files or any use of the district's NIS systems. The district reserves the right to monitor, track, log and access 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 established Board policy, software blocking or online server blocking. Specifically, the district operates and enforces technology protection measure(s) that monitor and track 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 of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory,

threatening, harassing, discriminatory, violent, bullying, terroristic, and advocates the destruction of property.[3][4][10][11][12][13][14][15]

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.[10]

Upon request by students or staff, the Superintendent or designee may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.[3][16]

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 brought onto district property, or to district events, connected to the district network, containing district programs or district or student data (including images, files, and other information) in order to ensure compliance with this policy and other policies, to protect the district's resources, and to comply with law.[17][18]

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:

1. Highest – uses that directly support the education of the students.
2. Medium – uses that indirectly benefit the education of the students.
3. Lowest – uses that include reasonable and limited educationally-related interpersonal communications.
4. Forbidden – all activities in violation of this policy.

The district additionally reserves the right to:

1. Determine which NIS systems' services will be provided through district resources.
2. Determine the types of files that may be stored on district fileservers and computers.
3. View and monitor network traffic, fileserver space, processor, and system utilization, and all applications provided through the network and communications systems, including email and other electronic communications.
4. Remove excess email or files taking up an inordinate amount of fileserver disk space after a reasonable time.
5. Revoke user privileges, remove user accounts, or refer to legal authorities when violation of this and any other applicable 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.

Delegation of Responsibility

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

The district shall inform staff, students, parents/guardians and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.[10]

Users of the district's NIS systems or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

Student user agreements shall also be signed by a parent/guardian.

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

The Director of Technology or designee will establish a process for setting up individual and class accounts; develop best practice guidelines for users to manage their email boxes and network folders; set quotas for disk usage on the system; establish a district electronic document retention policy, document destruction policy, and document retention schedule; and establish the district's 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.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:[3][4][19]

1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Board.

2. Maintaining and securing a usage log.

3. Monitoring online activities of minors.

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:[4]

1. Interaction with other individuals on social networking websites and in chat rooms.

2. Cyberbullying awareness and response.[15][20]

Guidelines

All data files created, transmitted, or stored on district equipment are the property of the district and are not protected by any right to privacy; provided, however, that (1) student information protected by the Family Educational Rights and Privacy Act (FERPA) or other federal or state statute(s) requiring confidentiality will be treated as confidential according to the terms of the statute(s); and (2) that student work may be subject to protection under copyright law.[21][24][25]

No confidential data shall be transmitted from a Neshaminy School District network, unless permitted by applicable law or until appropriate permissions are received according to the law.

The district declares that its computer resources, computer networks, social media, web page, and related facilities are not a public forum, and reserves the right to deny access to any user whose use would serve to establish a public forum.

No employee or student using Neshaminy School District technology, which shall include software, hardware and data derived from use of the computer network, shall have any right of privacy or

expectation of privacy with respect to anything done with said technology. The technology belongs to, is licensed to, or is accessible through technology that is owned by or licensed to Neshaminy School District. Neshaminy School District retains all rights as an owner or licensee with respect to all technology that it owns or licenses and has, unless restricted by an express agreement with a third party supplier, the rights of an owner or licensee, including, the rights to use, transfer, inspect, copy, delete, read, or store any such technology.

Parental Notification and Responsibility

The district will notify parents/guardians about the district NIS systems and the policies governing their use. 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/guardians bear primary responsibility for transmitting their particular set of family values to their children. The district will encourage parents/guardians 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/Guardians are responsible for monitoring their children's use of the district's NIS systems when they are accessing the systems from outside of the 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 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 it. 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 in this policy. The district reserves the right to determine if any activity not stated in this policy 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.

General Prohibitions –

Users are prohibited from using district NIS systems to:

1. Communicate about nonwork or nonschool-related communications using district-assigned email accounts.

    a. District employees may be allowed to access their personal ISP email accounts through the Internet, provided it does not interfere with their job responsibilities and with other employee job-related use of computer and network resources.

b. Students may be allowed to access their personal ISP email accounts through the Internet, provided it is not done on class time and it does not deny other students of computer and network resources.

c. Examples of personal ISP accounts are AOL, Comcast, Verizon, Hotmail, Yahoo and Gmail.

2. 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.

3. 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, violent, vulgar, rude, inflammatory, threatening, profane, pornographic, offensive, terroristic and/or illegal.

4. Bully/Cyberbully another individual.[15][20]

5. Access or transmit gambling or pools for money, including but not limited to basketball and football, or any other betting or games of chance.

6. 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.

7. Send terroristic threats, hate mail, harassing communications, discriminatory remarks, and offensive or inflammatory communications.

8. Participate in unauthorized Internet Relay Chats and instant messaging communications (online, real-time conversations) that are not for school-related purposes or required for employees to perform their job duties.

9. Facilitate any illegal activity.

10. Communicate through district email for noneducational purposes or activities. The use of email to mass mail noneducational or nonwork-related information is expressly prohibited (for example, the use of the "everyone" distribution list, building level distribution lists, or other email distribution lists to offer personal items for sale is prohibited).

11. Engage in commercial, for-profit, or any business purposes (except where such activities are otherwise permitted or authorized under applicable district policies); conduct unauthorized fundraising or advertising on behalf of the district and nonschool 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.

12. Engage in political lobbying.

13. 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.[21]

14. 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.

15. 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

protect the confidentiality of sensitive or critical information in the district's approved manner.

16. Access, interfere, possess, or distribute confidential or private information without permission of the district administration. An example includes accessing other students' accounts including, but not limited to, obtaining personal demographics, grades, library or lunch accounts.

17. Violate the privacy or security of electronic information.

18. 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.

19. Send unsolicited commercial electronic mail messages, also known as spam.

20. Post personal or professional web pages without administrative approval.

21. Post anonymous messages.

22. Use the name of the 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 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.

23. 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.

24. Advocate illegal drug use, whether expressed or through a latent pro-drug message. This does not include a restriction of political or social commentary on issues, such as the wisdom of the war on drugs or medicinal use.

25. 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.

Users are not permitted to have blogs without the review and approval of the Superintendent or designee and building principal. All bloggers must follow the rules provided in this policy and other applicable policies, administrative regulations and rules of the district.

Access and Security Prohibitions –

Users must immediately notify the Director of Technology or designee if they have identified a possible security problem. The following activities related to access to the district's NIS systems and information are prohibited:

1. Misrepresentation (including forgery) of the identity of a sender or source of communication including, but not limited to, spoofing and phishing.

2. 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.

3. Using or attempting to use computer accounts of others; these actions are illegal, even with consent, or if only for the purpose of "browsing".

4. 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.

5. Disabling or circumventing any district security, program or device including, but not limited to, anti-spyware, anti-spam software, and virus protection software or procedures.

6. 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 and control of the district; for example, working at home, on vacation or elsewhere. If any user becomes aware of the release of district information, data or records, the release must be immediately reported to the Superintendent or designee. At the direction of the Superitendent or designee, the Director of Technology will analyze the breach to determine its scope.[22]

Operational Prohibitions –

The following operational activities and behaviors are prohibited:

1. 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. The 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".

2. Altering or attempting to alter files, system security software or the systems without authorization.

3. Unauthorized scanning of the NIS systems for security vulnerabilities.

4. 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.

5. Unauthorized wiring, including attempts to create unauthorized network connections, or any unauthorized extension or retransmission of any computer, electronic communications systems, or network services, whether wired, wireless, cable, or by other means.

6. Connecting unauthorized hardware and devices to the NIS systems.

7. 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.

8. Intentionally damaging or destroying the integrity of the district's electronic information.

9. Intentionally destroying the district's computer hardware or software.

10. Intentionally disrupting the use of the NIS systems.

11. Damaging the district's NIS systems or networking equipment through the users' negligence or deliberate act.

12. Failing to comply with requests from appropriate teachers or district administrators to discontinue activities that threaten the operation or integrity of the NIS systems.

<u>Electronic Mail</u>

Neshaminy recognizes that the use and access of personal e-mail accounts by staff may be an acceptable use when such use supports the instructional program or supports the professional and/or personal needs of staff. Students may access personal email accounts only when that access supports a legitimate educational use and is approved by a teacher .

Social Media

As used in this policy, **social media** includes a blog, wiki, Facebook, Twitter, Ning or any Internet-based network that allows virtual contact between users. **Social networks** are forums for sharing information. Neshaminy School District distinguishes between two (2) uses of social media – those used to support the learning and business needs of the school district, and social media that is used by individual employees of the district.

Organizational Guidelines

Social media, professional networking sites, rapid-fire communications, blog sites, and program-specific websites are all useful technologies. When sponsored and used in Neshaminy, these technologies must serve the district's unique needs, align with the district's goals and objectives, and be consistent with Neshaminy School District Board policy and administrative regulations. Such social media sites must also adhere to all applicable federal, state, and local laws, regulations, and policies, including, but not limited to, those addressing individual privacy and confidentiality.

The Director of Information Technology or his/her designee shall approve all social media sites representing Neshaminy. The department or program that operates a Neshaminy social media site is responsible for the content of that site.

All employees authorized to post on behalf of Neshaminy on such social media sites will be approved, trained on this policy, and have appropriate content and technical expertise. The Director of Information Technology and his/her designee shall monitor all Neshaminy social media sites. Neshaminy reserves the right to remove any content that is deemed in violation of any applicable policy of the school district or any applicable law.

Personal Social Media

Employees who communicate electronically with students should only conduct such communication through approved Neshaminy equipment/software and via approved communication vehicles, such as a district-developed social networking page. When working on the Neshaminy network, employees are prohibited from communicating with students via personal social media. Employees of the Neshaminy School District are strongly discouraged from communicating with students via a personal social media page or with personal equipment/software; i.e., cell phone, home phone, home computer, etc. using social media software/technologies on personal or private networks. Employees are also discouraged from communicating with parents/guardians through social media. It is recognized, however, that contacts with parents/guardians by cell phone is an acceptable use when the phone contact, by call or text, meets the legitimate needs of the employee in communicating school-related information to the parent/guardian.

The use of social media by any employee or student, such as, but not limited to, blogging, texting, tweeting, and/or instant messaging, in ways that are contrary to the district's policies or are illegal or violate antidiscrimination policies will be subject to disciplinary action.

Copyright Infringement and Plagiarism

The illegal use of copyrighted software by students and employees is prohibited.

Any data uploaded or downloaded to or from the Internet shall be subject to fair use guidelines.[21]

Federal laws, cases and guidelines pertaining to copyright will govern the use of material accessed through district resources. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct other users to respect copyrights, request permission when appropriate, and comply with license agreements. Employees will respect and comply as well.[21][23]

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.

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' websites.

Further, the illegal installation of copyrighted software or files for use on the district's computers is expressly prohibited. This includes all forms of licensed software – shrink-wrap, clickwrap, browsewrap and electronic software downloaded from the Internet.

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

Board policies on the selection of materials will govern use of the district's NIS systems.

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 websites they require or recommend students access to determine the appropriateness of the material contained on or accessed through the website. 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.

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 Superintendent or designee.

Consequences for Inappropriate, Unauthorized and Illegal Use

Among other consequences for a violation of this policy, users, including students or employees, shall be financially responsible for damages to the equipment, systems, software, and data files resulting from negligent, reckless, deliberate or willful acts or omissions. In addition, damaging, destroying or altering any computer, network equipment, or any data files may result in disciplinary action under this policy and under any other Neshaminy School District School Board policy applicable to the conduct. Unauthorized or illegal use of computers or computer networks; intentional deletion or damaging of data files; copyright violations or theft of services may result in disciplinary action under the provisions of this policy and/or under any other Neshaminy School District School Board Policy applicable to the conduct.[7][8][9]

Denial of computer and computer network access and other disciplinary actions including suspension, expulsion, termination of employment, and possible criminal penalties are part of the available consequences for inappropriate use.

Safety and Education

The district will take appropriate measures to prevent users of district technology from harassment or unwanted communication. Users who receive threatening or unwelcome communications while using district technology should report them immediately to a building administrator.

The district will take appropriate measures, through the use of hardware and/or software tools, in an effort to prevent any user from being exposed to graphic, text, and any other form of obscene, pornographic, or other material that is harmful to minors. This includes using one (1) or more Internet content-filtering agents that will remove and/or block Internet content.

Except as determined by the Director of Information Technology, these Internet content-filtering agents will not be deactivated for any Neshaminy user. Notwithstanding filter implementation, the user retains full responsibility for his/her use of Neshaminy technology.

The district will educate students about appropriate online behavior, including appropriate interactions with others on social networking sites and cyberbullying awareness and response.[4][15][20]

Legal

1. 18 U.S.C. 2256
2. 18 Pa. C.S.A. 6312
3. 20 U.S.C. 6777
4. 47 U.S.C. 254
5. 18 Pa. C.S.A. 5903
6. 18 U.S.C. 2246
7. Pol. 218
8. Pol. 233
9. Pol. 317
10. 24 P.S. 4604
11. Pol. 103
12. Pol. 103.1
13. Pol. 104
14. Pol. 218.2
15. Pol. 249
16. 24 P.S. 4610
17. Pol. 226
18. Pol. 237
19. 47 CFR 54.520
20. 24 P.S. 1303.1-A
21. Pol. 814
22. Pol. 830
23. 17 U.S.C. 101 et seq
24. Pol. 113.4
25. Pol. 216

24 P.S. 4601 et seq

Pol. 220