

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF
INTERNET AND
INFORMATION SYSTEMS

ADOPTED: March 10, 1997

REVISED: March 8, 2010

NORTHERN LEHIGH SCHOOL DISTRICT

<p>1. Purpose</p>	<p style="text-align: center;">815. ACCEPTABLE USE OF INTERNET AND INFORMATION SYSTEMS</p> <p>The Northern Lehigh School District and the Northern Lehigh School District’s Board of School Directors supports the use of technology, information systems (student, financial, data warehouse, etc.), electronic communication systems, local and wide-area networks and the Internet, including any equipment and/or devices or services associated with these technologies (collectively Information Systems), in the school district’s instructional program in order to facilitate teaching and learning.</p> <p>The Information Systems provide a wide range of diverse and unique resources which the school district provides to employees, students, School Board members, and guests (Users) to access information, conduct research, and facilitate collaboration in order to advance the district’s educational purpose and mission. Guests include, but are not limited to, visitors, workshop attendees or presenters, volunteers, independent contractors, consultants, adjunct education staff, substitute teachers, and visiting students.</p> <p>The school district’s Information Systems must only be used for education-related purposes and the performance of school district job duties by Users. Incidental personal use of school district computers is permitted for employees as long as such use does not interfere with the employee’s performance of job duties, Information Systems operations, and with ability of other Users to use or access the Information Systems. Personal use must comply with this policy, rules and procedures contained within this policy, and all other applicable school district policies, the Internet service providers (ISP) terms of use, local, state and federal laws and must not damage the school district’s Information Systems in any way. Students are permitted to use the Information Systems for educational purposes only.</p> <p>Personal technology devices or other electronic devices brought onto the school district’s property, or at school district events, or connected to the school district’s Network, that the school district reasonably believes may contain school district information or contain information that violates any school district policy, or contains any information/data that the school district reasonably believes involves criminal activity may be legally accessed to ensure the compliance with this policy, any other school district policies, and to comply with state and federal laws.</p>
-------------------	--

<p>18 U.S.C. Sec. 2256</p>	<p>Child Pornography - under federal law, child pornography is defined as a visual depiction of any kind, including a drawing, cartoon, sculpture, or painting, photograph, film, video, or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where it 1) depicts a minor engaging in sexually explicit conduct and is obscene, or; 2) depicts an image that is, or appears to be, of a minor engaging in graphic bestiality, sadistic or masochistic abuse, or sexual intercourse, including genital-genital, oral-genital, anal-genital, or oral-anal, whether between persons of the same or opposite sex, and such depiction lacks serious literary, artistic, political, or scientific value. (Section 2256 of Title 18, United States Code).</p>
<p>18 Pa. C.S.A. Sec. 6312</p>	<p>Under Pennsylvania law, 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.</p>
<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>Commercial Purposes - defined as offering or providing goods and/or services and/or purchasing goods/and/or services for personal use.</p> <p>Educational Purpose - includes the use of the Information Systems for classroom activities, professional or career development and to support the school district’s curriculum, mission, policy and strategic plan.</p> <p>Harmful to Minors - means any picture, image, graphic image file, or other visual depiction that:</p> <ol style="list-style-type: none"> 1. Taken as a whole and with respect to minors, appeals to a 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 a lewd exhibition of the genitals; and 3. Taken as a whole lacks serious literary, artistic, political, or scientific value as to minors. <p>Inappropriate Materials - inappropriate material includes, but is not limited to, visual, graphical, textual and any other form of obscene, sexually explicit, pornographic, child pornographic, or any other materials that may be harmful to minors, hateful, illegal, defamatory, lewd, vulgar, profane, inflammatory, threatening, harassing, discriminatory (as it pertains to race religion, color, national</p>

<p>18 Pa. C.S.A. Sec. 5903</p>	<p>Under Pennsylvania law (PA C.S.A. § 5903) , any material or performance, if:</p> <ol style="list-style-type: none"> 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 of a type described in this section. 3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.
<p>18 Pa. C.S.A. Sec. 5903 18 U.S.C. Sec. 2246</p>	<p>Sexual Act and Sexual Contact - the terms 'sexual act' and 'sexual contact' have the meanings given such terms in Section 2246 of Title 18, United States Code.</p>
<p>42 U.S.C. Sec. 254</p>	<p>Technology Protection Measures - means a specific technology that blocks or filters Internet access to visual depictions that are:</p> <ol style="list-style-type: none"> 1. Obscene, as that term is defined in Section 1460 of Title 18, United States Code. 2. Child pornography, as that term is defined in Section 2256 of Title 18, United States Code. 3. Harmful to minors.
<p>18 U.S.C. Sec. 2256</p>	<p>Visual Depictions - not limited solely to photographs, undeveloped film and video tapes, but includes images stored as data on computer disk or other storage device. Images stored by electronic means which are capable of being converted into a visual image. (United States vs. Hall, 142 F.3d 988, 998 (7th Cir. 1998).)</p>
<p>3. Authority</p>	<p>Access to the school district’s Information System through school district resources is a privilege not a right. School district resources, as well as, User accounts, data and information are property of the school district. The school district reserves the right to deny access to prevent unauthorized, inappropriate, or illegal activity or use, and may revoke those privileges and/or administer appropriate disciplinary action. The school district also reserves the right to determine which services will be provided through the Information Systems. The school district will cooperate to the extent legally required with an ISP(s), local, state and federal authorities in any investigation concerning or related to the misuse of the Information Systems and/or violation of any applicable laws or regulations.</p>

<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>In performing routine maintenance and security tasks it is often necessary for systems administrators to access User accounts. Systems administrators (i.e. Director of Technology or his/her designee) have the right to access by interception and/or access directly stored communications or data for any reason in order to uphold this policy and maintain the Information Systems. Users should have no expectation of privacy for the content of their personal files or their use of the school district's Information Systems. The school district reserves the right to monitor, track, log and access Information Systems use and to monitor and allocate fileserver and storage resources.</p> <p>Students and staff have the responsibility to respect and protect the rights of every other User in the district and on the internet/network/software, hardware, peripherals, and other information technology equipment.</p> <p>The school district reserves the right to restrict access to any Internet sites or functions that it deems inappropriate through general policy, software or on-line server blocking. The school district operates and enforces technology protection measures that monitor, block or filter on-line activities of Users which block and filter inappropriate material on the Internet and monitor all network activity. Measures used to restrict Users access to material that is harmful to minors may be disabled by an adult to access bona fide research material(s), not within the prohibitions of this policy or for another lawful purpose. No User may access material that is illegal under state or federal law. An expedited review and resolution of a claim that the Policy is denying a student or adult access to material will be enforced by an administrator, supervisor, or their designee upon the receipt of written consent from a parent or guardian for a student or upon the written request from an employee. The school district shall not be responsible for any unauthorized charges or fees resulting from Users accessing the Internet.</p> <p>The school district has the right, but not the duty, to monitor, track, log, access, and report all aspects of its Information Systems for all Users and any User's personal computers, peripherals, PDAs, electronic devices and media they bring onto school district property, or to school district events, that are/were connected to the school district network, which the school district reasonably believes may contain school district programs, or school district and/or student data (including images, files, and other information) all pursuant to the law, in order to insure compliance with this policy and any other school district policies, to protect the school district's resources and Information Systems and to comply with the local, state and federal laws.</p> <p>The school district reserves the right to restrict lower priority Information Systems and computer uses when network and computing requirements exceed available capacity according to the following priorities.</p>
---	--

<p>4. Delegation of Responsibility</p>	<ol style="list-style-type: none"> 1. <i>Highest</i> – uses that directly support the education of students. 2. <i>Medium</i> – uses that indirectly benefit the education of the students. 3. <i>Lowest</i> – uses that include reasonable and limited educationally-related interpersonal communications and incidental personal use. 4. <i>Forbidden</i> – any activities in violation of this policy or the local, state, and federal laws. <p>The school district also reserves the rights to:</p> <ol style="list-style-type: none"> 1. Determine which services will be provided through school district resources and Information Systems. 2. View, monitor, capture and archive any and/or all network activity. This may also include viewing and monitoring files server storage space usage, processor and system utilization, all services and applications provided through the Information Systems, including electronic mail, Internet messaging, and other means of electronic communications that currently exist or may exist in the future. 3. Limit the amount of User storage space allocated to personal files and/or e-mail. Remove e-mail and/or personal files taking up an excessive amount of storage space after a reasonable amount of time. 4. Revocation of User privileges, removal of User accounts, or referral to legal authorities when a violation of this policy or any other applicable school district policies takes place or state or federal laws are violated, including, but not limited to, those governing network use, copyright, security, privacy, employment or destruction of school district property. 5. Add or change policy, rules, regulations, and restrictions at anytime regarding access and use of the school district’s Information Systems. <p><u>School District</u></p> <p>Because the Internet is a global network linking millions of computers and thousands of networks around the world with no one organization or governing body controlling it, inappropriate material may be accessible through the school district’s Information Systems and Electronic Communications Systems. Because of the nature of the Internet to be ever changing it is virtually impossible to completely block access to all these resources. Accessing these and similar types of resources</p>
--	--

may be considered a unacceptable use of school district resources and will result in actions outlined in the Consequences for Inappropriate, Unauthorized and/or Illegal Use section of this policy and as provided in other applicable and relevant school district policies. The school district will make reasonable efforts to ensure that its educational resources are used responsibly by students and staff.

The Superintendent or his/her designee has the following responsibilities:

1. Provide for systems and procedures to monitor, track, log, access, and report sufficient aspects of the school district's Information Systems that may need to be inspected pursuant to provisions of applicable local, state, or federal laws, to endure compliance with this policy or any other applicable school district policies, and to protect the school district's Information Systems and resources.
2. Defining and setting usage limits or quotas to ensure optimal use of the Information Systems according to the following priorities:
 - a. Uses that directly support educational activities of students.
 - b. Uses that indirectly benefit the education of students, such as researching career or college information.
3. Ensure the security of personal and confidential data maintained in the student information system, financial information system and any other systems that may be acquired and implemented by the school district.
4. Reserves the right to:
 - a. View, monitor, capture, and archive all network and e-mail communications.
 - b. View and monitor file server storage space usage, processor and system utilization, all applications provided through the Information Systems, including e-mail.
 - c. Maintain e-mail and file server storage quotas.
 - d. Revoke User privileges, remove User accounts, or refer to legal authorities when a violation of this policy and/or any other applicable school district policies occur or local, state, or federal law is violated.
 - e. Determine which technology services will be provided through the school district Information Systems.

	<p>The Director of Technology or his/her designee will serve as coordinator to oversee the school district's Information Systems and will cooperate with district, regional, and state organizations as necessary to educate employees, approve activities, provide leadership for proper training for all Users in the use of the Information Systems and requirements of this policy, establish procedures and systems to ensure sufficient supervision of the Information Systems, and interpret and enforce this policy.</p> <p>The Director of Technology or his/her designee will setup and maintain a procedure for creating and assigning individual and class User accounts, set quotas or limits for usage of disk storage and e-mail storage, setup and maintain a system for the archiving of school district and individual data stored on school district file servers or other electronic storage facilities, maintain a virus protection process.</p> <p>The Director of Technology or his/her designee will establish network authentication requirements which meet the following criteria:</p> <ol style="list-style-type: none">1. The employee's password must be at least eight (8) characters in length of mixed alphabetic and numeric characters containing at least one (1) upper-case alphabetic character.2. The employee's password must be changed every thirty (30) days.3. The employee will be locked out of their network/student information system account after three (3) unsuccessful login attempts. <p>Employees will be required to follow these network authentication requirements which may change at any time due to the security requirements of the school district.</p> <p><u>Users</u></p> <p>Employees must be proficient in their ability to use the school district's Information Systems and any software relevant to their job responsibilities. Additionally, they must practice proper network etiquette, school district ethics, and agree to the requirements of this policy.</p> <p>Etiquette – All Users are expected to abide by generally accepted rules of network etiquette which include, but are not limited to, the following:</p> <ol style="list-style-type: none">1. Be courteous. Do not send messages containing inflammatory or antagonistic criticism or abusive, insulting or threatening remarks. They also should not contain vulgarities and other inappropriate language. General school district policies and rules for behavior and communicating apply.
--	--

<p>5. Guidelines</p>	<ol style="list-style-type: none"> 2. Do not reveal the personal information or personal information of others such as addresses or telephone numbers. 3. Remember that network communications such as e-mail is not necessarily private. 4. Do not use the Internet or e-mail in any way that would interfere with or disrupt its use by other Users. 5. Consider all communications, data and information stored or accessible on the school district's Information Systems as school district property. 6. Respect the rights of others to have access and use of an open and hospitable technology environment regardless of their race, ethnicity, color, religion, creed, age, sexual orientation, marital status, handicap or disability. <p>Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.</p> <p>Students and staff have the responsibility to respect and protect the rights of others to have access and use of an open and hospitable technology environment.</p> <p>Teachers shall guide students in determining educational appropriateness. The Principal shall have the decision-making authority to determine what is inappropriate.</p> <p><u>Access To The Information Systems</u></p> <p>The school district network, e-mail or other accounts will be used only by the authorized owner of the account for its authorized purpose. Accounts will be made available according to a schedule developed by appropriate district authorities. Accounts will be given out to only those individuals who meet the following requirements:</p> <ol style="list-style-type: none"> 1. Have read the district Acceptable Use Policy (this policy) with its provisions and acknowledge this by signing the Acceptable Use Policy Acknowledgement Form and returning it to the appropriate district authority. Students must have their parent/guardian sign this signature page indicating the parent's/guardian's receipt of the policy. Staff members must sign this form and also return it to the appropriate district authority.
----------------------	--

2. Have received instruction which will include but not be limited to instruction on network access, use, acceptable vs. unacceptable uses, network etiquette, and the consequences of abuse of privileges and responsibilities. This requirement shall apply for both students and district employees.

This policy as well as other applicable school district policies will govern the use of the school district's Information Systems for Users. User's use of the Information Systems will also be governed by other relevant school district policies as well as local, state, or federal law.

Types of services include, but are not limited to:

1. World Wide Web (Web) – All Users will have access to the Web as needed. Access to information on the Web will be subject to technology protection measures. The school district reserves the right to monitor, view, capture, and archive any and/or all usage of this service.
2. Electronic Mail (e-mail) – school district employees and School Board members will be provided with individual e-mail accounts for work and school district related business use as needed.
3. Guest Accounts – Guest Accounts are Information Systems accounts to any of our various systems that are given to Guests for a specific school district-related purpose. These accounts may be long standing permanent accounts or short-term accounts that have limited time duration associated with them. Guest accounts will be setup only with the approval of the Director of Technology or his/her designee. The use of these accounts by a Guest is governed by this policy, any other applicable school district policy, or local, state or federal law. A signed Acceptable Use Policy Agreement is required if this account is assigned to an adult and a parent/guardian signature is required if this account is assigned to a minor.
4. Web Logs (Blogs) – school district employees may be permitted to have school district-sponsored Blogs after they receive approval from the school district and the appropriate training. Bloggers must follow the rules provided in the Policy and any other applicable school district policies, rules and regulations.
5. Second Generation Web-based Services (Web 2.0) – The school district may authorize that certain Web 2.0 services, such as, but not limited to, wikis, social networking sites, folksonomies, RSS feeds, course management systems and collaboration tools, that enable on-line educational collaboration between Users be permitted by the school district for education-related use; however such use must be approved by the Superintendent and his/her designee, followed by

relevant training authorized by the school district. User must follow the rules provided in the Policy and any other applicable school district policies, rules and regulations.

6. Next Generation Web Services and beyond – The school district may authorize that certain web or Internet based services that become available in the future,, be available to Users for education-related use; however such use must be approved by the Superintendent and his/her designee, followed by relevant training authorized by the school district. User must follow the rules of this policy and any other applicable school district policies, rules and regulations.

Access to all data on, taken from, or compiled using school district computers is subject to monitoring, inspection, and discipline. Users have no right to expect that the placement of school district data and/or information on User's personal computers, networks, Internet, electronic communication systems, and storage media is not beyond the access of the school district. The school district reserves the right to legally access User's personal technology devices brought onto the school district property, or to a school district event, or connected to the school district's network, when school district reasonably believes they contain school district information, or contains information that violates any school district policy, or contains any data/information that the school district reasonably believes may violate local, state, or federal law or involves criminal activity of any kind.

Parental Notification And Responsibility

The school district will notify parents/guardians about the district's Acceptable Use Policy # 815 (this policy) at the beginning of every school year. This policy will be published in every student handbook and posted on the school district's website. Additionally, parents/guardians will be required to agree to and sign the school district's Acceptable Use Policy Acknowledgment Form. The school district recommends that the parent/guardian read over this policy carefully and discuss it with their child(ren) as to what material is and is not acceptable for their child(ren) to access through the school district's Information Systems.

School District Limitation Of Liability

The school district makes no expressed or implied warranties, endorsements, or guarantees, of any kind, that the information, content, functions, or services provided by or through the school district's Information Systems will be error free or without defect nor does the school district guarantee the accuracy or quality of information obtained or received from the Internet. The school district does not warranty or guarantee the effectiveness of Internet content filtering. The availability of electronic information to Users does not imply endorsement of the content by the school

district. The school district shall not be responsible for any damages Users may suffer, including but not limited to, information that may be lost, damaged, delayed, or unavailable when using the school district's Information Systems. The school district shall not be responsible for any unauthorized financial obligations, fees, or charges resulting from access to the school district's Information Systems. In no event shall the school district be liable to the User for any damages, direct or indirect, special, or consequential arising from the use of the school district's information systems.

Prohibitions

The use of the school district's Information Systems by Users for illegal, inappropriate, unacceptable, or unethical purposes is prohibited. The school district reserves the right to determine if any activity or use not appearing in the list of General Prohibitions constitutes acceptable or unacceptable use of the school district's Information Systems.

These prohibitions are in effect anytime school district resources are accessed whether on school district property, when using mobile computing equipment, other telecommunications facilities outside of the school district that is unprotected, directly from home, or indirectly through another ISP, and if applicable, when an employee or student uses their personal equipment.

Students are prohibited from using any of their own personal computing and/or electronic devices; including but not limited to, notebook, laptop, tablet PCs, PDAs, or other such devices as described in the definitions section of this policy as a computer; on school district property (this would include, but not be limited to, buses, vans or other vehicles), or at any school district events, or connected to the School Information Systems, either wired, wireless or by any other means, unless permission has been granted to do so by the Director of Technology and/or his/her designee, who will then assume responsibility to supervise the student usage, unless required as part of an IEP, in which case an employee will supervise the student usage. Users are prohibited from using cellular telephones with or without Internet access and/or recording and/or camera/video, and other capabilities. Users are prohibited for using cellular telephones with cameras or other digital cameras, or recording devices to take images of others, transfer them, or place them on web sites without consent of the building administrator. Students who are members of a volunteer fire company, ambulance, or rescue squad and performing those functions or need a computer due to a medical condition or disability, or the medical condition of a member of their immediate family with notification and approval of the school administrator may qualify for an exemption to this prohibition.

General Prohibitions

Users are prohibited from using the school district's Information Systems and/or personal electronic devices to:

1. Non-work or non-school related communications, unless for incidental personal use as defined by this policy.
2. Send, receive, view, download, access or transmit inappropriate material as described in the definitions section of this policy or advocate destruction of personal property.
3. Send, receive, download access, or transmit inappropriate material and material that is likely to be offensive or objectionable to recipients.
4. Cyberbullying of an individual.
5. Access or transmit gambling, pools for money, or any other betting or games of chance.
6. Access, read, or post in any news groups that deal with inappropriate and /or objectionable topics or materials, including those that conform to the definition of inappropriate material in the definitions section of this policy.
7. Use e-mail to send terroristic threats, hateful messages, harassing communications, discriminatory remarks, and offensive, profane, antagonistic, or inflammatory communications.
8. Participate in unauthorized Internet Relay Chats (IRC), instant messaging, and internet voice communications (on-line in 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 e-mail for non-educational, non-school related purposes or activities, unless it is for an incidental personal usage as defined in this policy. The mass e-mailing of non-educational, non-school related information is expressly prohibited except where the mailing is approved by the Superintendent or his/her designee for such things as community related events and announcements. Examples allowable e-mails would be an announcement for a fundraiser for the Slatington Public Library or a community benefit to help

<p>Pol. 814</p>	<p>someone in need. Example of prohibited e-mail would be the sale of personal items or the announcement of a special offer made by a local business that was not for the benefit of the school district.</p> <p>11. Engage in commercial, for-profit or any business purposes, except where such activities are otherwise permitted or authorized under this or other applicable school district policy. This would include conducting unauthorized fundraising; or advertising on the behalf of non-school organizations, except as approved by the Superintendent or his/her designee as discussed in the item above; reselling of district computer resources to an individual or organizations; use of the school district's name in any unauthorized manner that would reflect negatively on the school district, it's employees, or students.</p> <p>12. Political lobbying and lobbying for the purpose of electing public officials.</p> <p>13. Copy, install, and distribute copyrighted software not licensed by the school district on the school district's computers or copy school district licensed software to unauthorized systems. Prohibit any violation of copyright, or otherwise use another person's intellectual property without that individual's prior written approval or authorization; and downloading software must be with expressed approval from a supervisor (building principals for students) and when such occurs, such computer should have virus protection software running. Please see Policy 814 Copyrighted Material.</p> <p>14. Install computer hardware, peripheral devices, network hardware or any software on any school district-owned computer system or attach to any school district-owned network. Authority to install such hardware, devices, and software is restricted to the Director of Technology or his/her designee.</p> <p>15. Encrypt messages, send encrypted messages or encrypt files using any software that is not authorized by the school district from any point of access to the school district's Information Systems.</p> <p>16. Use the e-mail system or Information Systems to subscribe or to solicit information which incurs any form of cost without the expressed permission of a supervisor (building principals for students).</p> <p>17. Intentionally obtain or modify files, passwords, and data belonging to other Users.</p> <p>18. Alter a communication originally received from another User, individual or computer with the intent to deceive or defraud.</p>
-----------------	--

	<ol style="list-style-type: none">19. Store, install or use unauthorized games, programs, files, or other electronic media whether on individual school district computers or on any fileserver or other school district-owned storage device or appliance.20. Intentionally disrupt the work and/or education of other Users.21. Impersonate another User or sending any communication anonymously or under an alias unless authorized by the school district.22. Disable or circumvent any district security program or device this includes, but is not limited to, anti-virus software, anti-spam software, anti-spy ware software or system protection software.23. Bypass or attempt to bypass Internet content filtering software by any means or methods, including but not limited to use of anonymous proxy servers or use of a website that masks the content of a website from the content filter.24. Attempt to switch, destroy, modify, vandalize, or abuse any school district-owned Information Systems equipment, software, computer systems, or peripheral devices.25. Access, possess, or distribute confidential or private information unless it is within the scope of the position's job responsibilities.26. Send any school district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the school district's business, educational interests, or required by state or federal law.27. Post personal or professional web pages on a school district sponsored web site without administrative approval.28. Use school district-owned Information Systems or equipment to conduct denial of service attacks on school district or other systems.29. Quote personal or confidential communications in a public forum without the original author's prior consent.30. Use or attempting to use Information Systems accounts of others.31. Send unsolicited commercial mass e-mail messages (Spam).
--	--

32. Use the name of Northern Lehigh School District in any form on websites, web pages, blogs, discussion boards or forums not owned or related to the school district to express or imply the position of Northern Lehigh School District without the written permission of the Superintendent. When permission is not granted, the posting must state that the statement does not represent the position of Northern Lehigh School District.

33. Post anonymous messages.

Access And Security Prohibitions

Users must immediately notify the Director of Technology or his/her designee if they have identified a potential security problem or have inadvertently accessed inappropriate material. The following activities related to access to the school district Information Systems and information are prohibited:

1. Misrepresenting, including forgery of, the identity of a sender or source of communication.
2. Attempting to acquire or acquiring the passwords of another User. Accessing Information Systems by logging in using another Users account and password.
3. Sharing or knowingly allow your Information Systems accounts to be used by unauthorized Users. This would include posting User account names and/or passwords where they are unprotected and accessible to other Users.
4. Alter a communication originally received from another User, individual or computer with the intent to deceive or defraud.
5. Using the school district's Information System to commit an illegal act, including but not limited to, arranging for the sale of illegal drugs or the purchase or procurement of alcohol, any type of criminal activity, making or being involved in terroristic threats against any person or property.
6. Disabling or circumventing or attempting to defeat any school district security measure, program, or device. Circumventing or attempting to circumvent the school district's Internet content filtering.

Operational Prohibitions

The following operational activities and behaviors are prohibited:

1. Interfering with or disrupting the school district Information Systems including, but not limited to, transmission of computer viruses, worms, Trojan horses, trap door program code; sending of electronic mail designed to disrupt the e-mail system; and sending a large number of broadcast messages intended to choke network bandwidth. Users may not hack, attempt to hack, crack or attempt to crack into Information System resources such as file servers, applications, network devices, etc. using hardware and/or software of any kind to steal school district and/or User information, damage or disable Information Systems equipment or individual network components or capture information from data packets being transported across the district's network, take control of a User's computer remotely, or just to look around the network or Information Systems.
2. Scanning network or Information Systems for security vulnerabilities using any type of hardware and/or software devices.
3. Attempt to alter or alter any, but not limited to, files, security software, systems, file servers, switches, routers, computers, printers, and wireless access points beyond one's level of authorization or without proper authorization.
4. Connecting any unauthorized devices, hardware or combination of hardware and software to the Information Systems whether by directly wiring it to any network component, through wireless access to the Information Systems or through any other means.
5. Loading or downloading or the use of any unauthorized files or programs, including, but not limited to games, or use of any unauthorized electronic media.
6. Intentionally destroying the integrity of the school district's Information Systems.
7. Intentionally destroying or vandalizing the school district's Information Systems including but not limited to computers, printers, scanners, monitor, data projectors, keyboards, mice and software.
8. Damaging or disrupting the school district's Information Systems or network through a User's deliberate act or negligence.

<p>Pol. 814</p>	<p>9. Non-compliance with the requests from teachers and/or school district administrators to discontinue activities that the teachers or administrators believe to threaten the operation or integrity of the school district's Information Systems.</p> <p><u>Selection Of Materials</u></p> <p>Board policies on the selection of materials will govern use of the school district's Information Systems.</p> <p>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.</p> <p>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.</p> <p><u>Copyright Infringement And Plagiarism</u></p> <p>Federal laws, cases, and guidelines pertaining to copyright will govern the use of material accessed through the school district's Information Systems. Users will make a standard practice of requesting permission from the holder of the work and complying with license agreements. Employees will instruct students to respect copyrights, request permission when appropriate, and comply with license agreements. It is expected that employees will respect and comply as well.</p> <p>Violations of copyright law can be a felony. The law allows a court to hold individuals personally responsible for infringing the law. The school district does not permit illegal acts pertaining to the copyright law. Therefore, any User violating the copyright law does so at his/her own risk and assumes all liability.</p> <p>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 school district's computers is expressly prohibited. This includes all forms of licensed software.</p>
-----------------	--

<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p><u>Privacy, Search And Seizure</u></p> <p>The violation of this policy, any other applicable school district policy, local, state or federal law by a User may be discovered through routine maintenance or monitoring of the school district's Information Systems. The User waives all expectations of privacy by using the school districts Information Systems.</p> <p>The school district reserves the right to monitor, track, log, capture, archive, and access any electronic communication that traverses the school districts Information Systems, including but not limited to, Internet access, e-mails, instant messaging, or any other collaboration tools or programs that may be used at any time for any reason. As mentioned in the previous paragraph the User should not have any expectation of privacy in their use of the school district's Information Systems and other school district technology, even when it is being used for personal reasons. The school district has the right, but is not obligated, to legally access User's personal computers, peripherals, PDAs, and media they bring onto school district property, or to school district events, that are/were connected to the school district network, which the school district reasonably believes may contain school district programs, or school district and/or student data (including images, files, and other information) all pursuant to the law, in order to ensure compliance with this policy and any other school district policies, to protect the school district's resources and Information Systems and to comply with local, state and federal laws.</p> <p><u>Due Process</u></p> <p>The school district will cooperate with the school district's ISP's rules, terms and conditions, local, state, and federal authorities to the extent legally required in investigations concerning or relating to the use of the school district's Information Systems in any criminal or illegal activities.</p> <p>Users that possess due process rights for discipline resulting from the violation of this policy, whether by law or contractual agreement, will be accorded such rights.</p> <p>The school district may terminate the Information Systems and account privileges of a User by providing notice to that User.</p> <p><u>Safety And Privacy</u></p> <p>To the extent legally required the school district will take reasonable measures to protect Users from harassment or commercially unsolicited electronic communications. Any User who receives threatening or unwelcome communications must report them immediately to the Director of Technology or his/her designee.</p>
---	--

<p>Pol. 218, 233, 237, 248, 249, 317, 348, 417, 448, 517, 548, 814</p>	<p>Users may not post personal contact information about themselves or other persons on the school district's Information Systems. Users may not steal another User's identity in any way, may not use software, hardware devices, school district or personal employee technology or resources to invade one's privacy. Users may not disclose, use or disseminate confidential or personal information about students or employees, in either electronic or printed form, unless legitimately authorized to do so.</p> <p>Student Users agree not to meet with anyone they have met on-line unless they have parental consent.</p> <p><u>Consequences For Inappropriate, Unauthorized, And/Or Illegal Use</u></p> <p>General rules for behavior, ethics, and communications apply when using the school district's Information Systems and information, in addition to the stipulations of this policy. Students and employees must be aware that violations this policy or other policies, or for unlawful use of the Information Systems, may result in loss of Information Systems 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 school 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.</p> <p>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.</p> <p>Violations as described in this policy may be reported to the school district, appropriate legal authorities, whether the ISP, local, state or federal law enforcement. The school district will cooperate to the extent legally required with the ISP, local, state, or federal authorities in all such investigations.</p> <p>Vandalism will result in cancellation of access to the school district's Information Systems and resources and is subject to discipline.</p> <p>Any unauthorized third party usage of the school district's Information Systems will be prosecuted to the full extent of the law.</p>
--	--

References:

State Board of Education Regulations – 22 PA Code Sec. 403.1

PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312

Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.

U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq.

Obscenity – 18 U.S.C. Sec. 5903

Sexual Abuse – 18 U.S.C. Sec. 2246

Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256

Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777

Internet Safety – 47 U.S.C. Sec. 254

Board Policy – 218, 233, 237, 248, 249, 317, 348, 417, 448, 517, 548, 814