

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 2

<p>3. Procedures</p>	<p><u>Terms Of Agreement</u></p> <p>The North Schuylkill School Board requires all users (administrators, teachers, support staff, students and guests) of the district’s computers, networks, and Internet access to read and accept the Terms of Agreement before signing the Acceptable Use Agreement. Failure to comply with the terms of this agreement could result in the cancellation of the user’s account and/or computer usage privileges. Students will also need signed parental permission to use the Internet.</p> <p><u>General Computer Usage</u></p> <p>The North Schuylkill School Board recognizes the role of information and technology in the academic community and in the larger society. It is the policy of the School Board to provide all students, faculty, and staff with access to a variety of technology resources and to provide opportunities for all members of the district community to learn to utilize these resources effectively and efficiently. In return, it is expected that technology usage will be conducted in legally and ethically appropriate ways. All technology resources will be used in accordance with established policies of the School Board and with any and all local, state, and federal laws, and/or guidelines governing the use of technology and its component parts. Implicit in this is the expectation that all students, faculty, and staff will utilize the technology resources of the district so as not to waste them, abuse them, or interfere with or cause harm to other individuals, institutions, or companies. Users are expected to balance their own needs against the needs and expectations of other users.</p> <p><u>Access</u></p> <ol style="list-style-type: none">1. Students and staff will have access to computers and the district network during the normal school day. Students will have access to computers after school hours if supervised by and at the discretion of a staff member. Staff will have access to computers after school hours if building access is available. Network accessibility may be restricted during off-school hours for maintenance purposes. Home access to school-based files and selected software programs is available during after school hours. Usage is limited to the number of home access licenses available. Home access can’t be granted once usage has reached maximum license capacity.2. Users will be issued individual accounts and network permissions by the North Schuylkill School District Technology Department staff according to need. Administrators, directors, teachers, office staff and students will have individual system accounts.
----------------------	--

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 3

Software And Hardware

1. District computers are configured and maintained for educational and administrative purposes only and should not be viewed as the personal equipment of the user. Therefore, the right is reserved to restrict the configuration and installation of software and hardware on all district computers.
2. Any software installed on district computers must be licensed in accordance with the law. A separate license must be purchased for each computer upon which the software is installed. A copy of all licenses must be forwarded to the Technology Department staff before installation. All software and hardware purchases must be authorized by the Technology Director.
3. Users may not make unauthorized copies of software that is copyrighted.
4. Users may not install any unauthorized games, programs, files, or other electronic media on district computers.
5. Users may not move or remove equipment or install hardware or software without authorization by the Technology Department staff.
6. Users may not attempt to repair hardware or purchase component parts without authorization by the Technology Department staff.
7. Users will allow authorized technicians access to district computers for purposes of repair or installation.
8. Users may not physically damage or destroy hardware or do so by the introduction of worms or viruses. Vandalism, including theft of computer components, will result in monetary damages paid by the perpetrator, as well as disciplinary action according to district policy.

System Security

1. Users may not modify technology resources, utilities, and/or configurations, or change the restrictions associated with their accounts, or attempt to breach any technology resources security system, whether with or without malicious intent.
2. Users may not attempt to crash a system, or exploit weaknesses in security. If students find weaknesses, they must be reported immediately to the classroom teacher. District employees must report security weaknesses to the Technology Department staff as soon as possible but no later than one (1) working day from the time of the discovery.
3. Users must immediately notify the Technology Department staff if they have

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 4

	<p>identified a possible security problem or possible virus intrusion. Users may not search for security problems; this may be construed as an illegal attempt to gain access.</p> <ol style="list-style-type: none">4. Users may not engage in malicious hacking, i.e. deliberately breaking into a system to alter or damage it or for the purpose of getting illegitimate access to resources or information.5. Users may not misuse technology resources in any way that materially impacts on the desired result of others.6. While using the district network, users will not disseminate or archive on district network resources or those external to the North Schuylkill School District network any identifying criteria about other users.7. Users are responsible for the use of their individual account and should take all reasonable precautions to prevent others from being able to use their account, including logging off when away from the computer, especially if the computer is in an educational or insecure workplace setting. Unless authorized, users should not provide their password to another person. Certain networked software applications may require the use of a user's password by a substitute who has been hired to and needs to perform the same tasks as the absent employee.8. Users may not use a computer that has been logged in under another student or employee's name.9. Users may not give others access (via password or other means) to computing resources to which they are not entitled.10. Users may not use someone else's password or log in to someone else's account without authorization, except as may be required for management of system resources.11. Users may not attempt to gain access to computing privileges or resources for which they are not authorized or via means not authorized.12. Users may not use the system in any way to impersonate another user or to hide their identity through the use of pseudonyms or anonymity.13. Administrative or office computers should be utilized for their intended functions and should not be available to other users for general or personal use.14. Users may not read, execute, modify, or delete any file belonging to someone else without explicit permission from the owner, even if the file is unprotected.
--	--

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 5

15. Users may not use a system for unauthorized purposes such as advertising for a commercial organization, running a business, or illegal activities.
16. Users may not create, display or transmit obscene, libelous, or threatening messages or materials on the district's computer equipment.
17. An authorized system administrator may remove or alter as necessary user files that threaten to interfere with the operation of the system or as needed for system maintenance such as files infected with a virus, unauthorized programs that have adverse effects to the infrastructure, or copyright infringements. The system administrator should make every effort to notify the user prior to such action to give the user opportunity to remove such files him/herself. It is recognized that there may be special cases where the threat to the effectiveness of system resources is so immediate that prior notification is not possible. Users should keep backup copies of critical files.
18. System users have a limited privacy expectation in the contents of their personal files on the district system. Users should be aware that their personal files are discoverable under state public records laws.
19. The use of personal (non-district) computers on the network will not be supported. Personal computers should be registered in the building office with appropriate serial numbers and ownership information. The district is not liable for any damage done to personal computers. District-owned components may not be installed in a personal computer.
20. Users may not create, implement, or host their own servers or services using district resources.

ACCEPTABLE USE OF THE INTERNET

System Security

20 U.S.C.
Sec. 6777
47 U.S.C.
Sec. 254

1. A commercial software filter has been implemented that blocks access for minors and adults on the Internet to web sites with visual depictions and text that are obscene, contain child pornography, are harmful to minors with respect to use by minors, or that are determined inappropriate for use by minors by the School Board. No guarantees are made that the filters will block one hundred percent (100%) of the offensive material one hundred percent (100%) of the time. No filtering system is one hundred percent (100%) effective, partially due to the vastness and volatility of the Internet, and partially because of the arbitrary nature of the categorization. The same filters will apply to elementary and secondary students and to the staff.
2. Site requests may be submitted to the Director of Technology for the purpose of

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 6

	<p>review to ascertain the educational value of a site blocked by the Internet filter. If sites of equal or greater value are available, blocked sites may remain inaccessible. The filter can be disabled for sites that are deemed valuable and unique to bona fide research for adults or for other lawful purposes. Sites may be blocked to preserve network resources or for security purposes.</p> <ol style="list-style-type: none">3. An Internet usage log will be maintained and secured. Online activities of users may be monitored.4. Students are prohibited from unauthorized disclosure or dissemination of personal identification, including but not limited to the student's first or last name, address, phone number, picture, or e-mail address.5. District employees are prohibited from the unauthorized disclosure or dissemination of information about students' records, including but not limited to the student's first or last name, address, phone number, picture, or e-mail address.6. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the district Acceptable Use Policy, the discipline policy, or the law.7. An individual search may be conducted if there is reasonable suspicion that a user has violated the law or the district policies. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation. <p><u>Inappropriate Access To Material</u></p> <ol style="list-style-type: none">1. Users may not use, attempt to use, or direct the use of the district Internet system to access material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). Under no circumstances will users access Internet sites or utilize any other technological devices such as but not limited to cell phones, pagers, wireless WAN cards or any Bluetooth devices for purposes of harassment, threats, doing harm or inappropriate or illegal activities while on school property, or accessing school resources locally or remotely, or engaging in a school-sponsored activity. Access to Internet sites will be monitored and logged. Violators may lose Internet privileges which could impact academic success or be subject to other disciplinary action based on the severity of the violation. Violators may also be subject to legal action.2. If a user inadvertently accesses such information, s/he must immediately disclose the inadvertent access in a manner specified by his/her teacher or building administrator. This will protect users against an allegation that they have intentionally violated the Acceptable Use Policy.
--	--

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 7

47 U.S.C. Sec. 254	<p><u>Web 2.0 (Interactive) Web Site Access</u></p> <ol style="list-style-type: none">1. Users at the secondary school level only may have access to Web 2.0 (interactive) web applications and other future/emerging technologies, such as but not limited to blogs, wikis, podcasts, social networking, social bookmarking, chats and message boards for purposes of instruction related to the curriculum. Users will access these sites for use as instructional tools only. Users will be directed to sites that utilize educational materials. Due to the nature of interactive web sites, access to these sites may result in exposure to inappropriate material that is not accessible to the Internet filter. Misuse of these sites as previously defined in “Inappropriate Access To Material” may result in disciplinary action and could impact academic success. Classroom teachers will be responsible for monitoring and reporting abuses. Access to an interactive web site will be blocked if it is in violation of the Children’s Internet Protection Act or any other local, state, or federal law with respect to the use of the Internet by minors.2. Teachers at the elementary level may utilize online chats, message boards and other current or future interactive Internet applications for educational purposes only. Elementary students may not be the administrator of such activities. <p><u>E-mail</u></p> <ol style="list-style-type: none">1. District employees may be provided with a district e-mail account to use for educational purposes or district-related business.2. Users will not use e-mail for personal advertisements or to forward jokes, chain letters, or other mass mailings that are not school-related or appear to be spam.3. Elementary and middle school students using the district network will not be provided with school e-mail accounts and are not authorized to access their personal e-mail accounts.4. High school students may be allowed to create an e-mail account for purposes of instructional access to web sites. Students will not have access to these e-mail accounts while using the district network.5. Users may not repost (forward) a message that was sent to them privately without the permission of the person who sent them the message.6. Users may not post private information about another person.7. Users may not knowingly or recklessly post false or defamatory information about a person or organization.
-----------------------	--

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 8

8. Users may not post any inappropriate material or material that could be construed as harassment, libel, or a threat of any sort.
9. Users may not use vulgar, abusive, profane or other offensive language on district e-mail.
10. Users may not discuss illegal activities on district e-mail.
11. Users may not send attachments that are not school-related.
12. Authorities may subpoena e-mail in the incidence of any legal action taken upon an individual.

Commercial Purposes

Users may not use the district Internet system for commercial purposes.

Commercial purposes are defined as offering or providing goods or services for personal use. District acquisition policies will apply to the district purchase of goods or services through the system.

Copyright Issues

1. Copyright laws will govern the use of material accessed through the district system. Users that violate copyright laws will be solely liable for such violations.
2. Users may not use or install unlicensed software on district computers.
3. Users may not violate the law by illegally duplicating software.
4. Users may not plagiarize. Teachers will instruct students in appropriate research and citation practices.
5. When using material (text, graphics, sound, movies) from the Internet which could not be considered fair use for educational purposes, the user must request permission from the creator of the material before duplicating said material in any way. All materials on the Internet are copyrighted, whether so stated or not.
6. Users may not download materials in any format that are copyrighted without permission from the copyright holder, unless it is so stated that the material is free to download and use.

Establishment Of Web Sites

1. The district web site has been established to develop web pages that present information about the district. The Technology Director, building administrators

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 9

	<p>or their designee will be responsible for the approval of information posted on the web site. All web pages will be posted at the discretion of and by the Technology Director, building administrators or their designee, unless otherwise stipulated by the Technology Director.</p> <ol style="list-style-type: none">2. District employees may not officially or unofficially represent the school district on non-district web sites. The North Schuylkill School District is not liable for information posted on a non-district site.3. Groups associated with the school district such as: PTA's, booster clubs, band associations or other associations representing school district activities, may not establish web sites representing any school district affiliated group without review by the Technology Director of all material to be posted before it is posted.4. Schools and classes may establish web pages that present information about the school or class activities or for educational purposes. Teachers are responsible for the content created by their students. Student-created web pages will be posted at the discretion of the classroom teacher and by the approval of the Technology Director, building administrators or their designee. Disclaimers may be required stating that "Opinions expressed on this web page shall not be attributed to the North Schuylkill School District."5. With the approval of the Technology Director, extracurricular organizations may establish web pages. Advisors to the activities will be responsible for the content. Material presented on the organization web page must relate specifically to organizational activities. Disclaimers may be required stating, "Opinions expressed on this page shall not be attributed to the North Schuylkill School District." The Technology Director, building administrators or their designee approve organizational web pages, unless otherwise stipulated by the Technology Director.6. Any links occurring on district web pages must be done in accordance with the law and must be linked to sites that have an educational purpose. No links may occur within frames. The linked web site must be identified due to copyright considerations. Links may not be identified with defamatory, slanderous, libelous, or inappropriate language. No attempt should be made to misrepresent the location of a link. When links are used on a district web page, a reference must be made that states that "the North Schuylkill School District is not responsible for information contained on linked sites."7. Users will not have access to posting information on the authorized district web sites, unless otherwise stipulated by the Technology Director. Web sites are subject to approval of the Technology Director, building administrators or their designee.
--	--

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 10

<p>Pol. 216</p>	<p>8. The Technology Director reserves the right to edit or remove any material posted to any of the authorized district web sites.</p> <p>9. Advertising for commercial, political, or religious purposes is prohibited on district web pages.</p> <p><u>Student Records</u></p> <p>1. Written permission from both the parent/guardian and the student must be obtained prior to placing any student photographs, artwork, writing, or other projects on a web site. The work must appear with a copyright notice prohibiting the copying of such work without express written permission. Any requests for permission to copy a student's work must be forwarded to the parent/guardian of that student. Personal contact information about any student will not be displayed as a matter of convention on an authorized district web site. This includes but is not limited to: the student's first or last name, address, phone number, picture, or e-mail address. Authorization is needed from the parent/guardian of the student and from the building principal, Director of Technology, and Director of Education to post any personal contact information on a district web site. Dissemination of student information will be in accordance with Board Policy 216.</p> <p><u>Freedom Of Speech When Using District Resources</u></p> <p>1. Students have the right to exercise freedom of speech, including the right of expression. Disclaimers may be required stating, "Opinions expressed on this web page shall not be attributed to the North Schuylkill School District."</p> <p>2. Threats or intimidating statements made with reference to any persons within or without the school district are prohibited from being posted on any district web site or resource. Any form of bullying, including electronic/cyber bullying, is prohibited.</p> <p>3. The expression, publication, or distribution of obscene, libelous or slanderous materials, or materials which encourage students to commit unlawful acts, violate lawful school district regulations, or cause material and substantial disruption of the orderly operation of the school district, are prohibited.</p> <p>4. Users may not use the district web site as a forum for criticism of school district policies.</p> <p><u>Network Etiquette</u></p> <p>Users will communicate in a courteous manner when dealing with other users on the</p>
-----------------	--

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 11

<p>Pol. 317, 417, 517</p>	<p>network and with regard to any problems encountered when using district resources.</p> <p><u>Political Activities</u></p> <p>Users may not use the district system for political lobbying.</p> <p><u>Illegal Activities</u></p> <p>Users may not use the district system to engage in any illegal activities.</p> <p><u>Selection Of Materials</u></p> <ol style="list-style-type: none">1. When using the Internet for class activities, teachers will select material that is appropriate for the age of the students and that is relevant to the course objectives. Teachers will preview the materials and sites they require. Teachers will provide guidelines and lists of resources to assist their students in their research activities. Teachers will assist their students in developing the skills to ascertain the truthfulness of information and to distinguish fact from opinion.2. Internet downloads will be restricted to those files that have an educational purpose within the guidelines of the curriculum or in accordance with the requirements of one's job position. <p><u>Actions Resulting From Policy Violations</u></p> <ol style="list-style-type: none">1. Deliberate and/or negligent abuse of the network, computing resources, or any other policy violations as defined herein could lead to disciplinary action as established by the School Board and/or loss of network and/or Internet privileges. Loss of network privileges could result in the failure to meet established academic requirements necessary for graduation or promotion. Employees who violate the Internet policy as stated herein are subject to disciplinary action as defined in Board Policy 417.2. Offenders may also be subject to criminal prosecution. Under Pennsylvania law, it is a felony punishable by a fine of up to \$15,000 and imprisonment of up to seven (7) years for any person to access, alter, or damage any computer system, networking, software or database, or any part thereof, with the intent to interrupt the normal functioning of an organization. Disclosing a password to a computer system, network, etc., knowingly and without authorization, is a misdemeanor punishable by a fine of up to \$10,000 and imprisonment of up to five (5) years, as is intentional and unauthorized access to a computer or alteration of computer software.
---------------------------	--

815. ACCEPTABLE USE OF NETWORKS, INTERNET, AND COMPUTING RESOURCES
AND CIPA COMPLIANT INTERNET SAFETY - Pg. 12

	<p>References:</p> <p>Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.</p> <p>Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777</p> <p>Internet Safety – 47 U.S.C. Sec. 254</p> <p>Board Policy – 216, 317, 417, 517</p> <p>Forms:</p> <p>North Schuylkill School District Permission Form- Student Pictures and Work on the World Wide Web</p> <p>North Schuylkill School District Acceptable Use of Networks, Internet, and Computing Resources- Elementary Schools</p> <p>North Schuylkill School District Acceptable Use of Networks, Internet, and Computing Resources- Junior Senior High School</p> <p>North Schuylkill School District Acceptable Use of Networks, Internet, and Computing Resources- Staff</p> <p>North Schuylkill School District Acceptable Use of Networks, Internet, and Computing Resources- Guests</p>
--	---