

SUSQUEHANNA COMMUNITY SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: COMPUTER AND INTERNET
ACCEPTABLE USE

ADOPTED: May 16, 2007

REVISED:

<p>1. Purpose</p> <p>2. Authority</p>	<p style="text-align: center;">815. COMPUTER AND INTERNET ACCEPTABLE USE</p> <p>The Board supports use of the Internet and other computer networks in the district's instructional and operational programs.</p> <p>The purpose of access to the Internet and other computer networks is to support education in and among the schools of the district by providing access to unique resources and the opportunity for collaborative work. The use of student and staff accounts must be in support of education and academic research and consistent with the educational objectives of the district. Use of other organization's networks or computing resources must comply with the rules and regulations for that network.</p> <p>The district makes no warranties of any kind, whether expressed or implied, for the service it is providing. The district will not be responsible for any damages users suffer through appropriate or inappropriate use of the district computer resources and Internet access. This includes loss of data resulting from delays, nondeliveries, misdeliveries, or service interruptions caused by system problems and/or failure, user negligence, errors or omissions. Use of any information obtained via the computer resources of the district is at the user's risk. The district specifically denies any responsibility for the accuracy or quality of information obtained through the Internet.</p> <p>The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.</p> <p>The district reserves the right to log network use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users.</p> <p>The Board establishes that use of the Internet is a privilege, not a right; inappropriate, unauthorized and illegal use will result in cancellation of those privileges and disciplinary consequences.</p>
---------------------------------------	---

815. COMPUTER AND INTERNET ACCEPTABLE USE - Pg. 2

<p>P.L. 106-554 Sec. 1732</p> <p>3. Delegation of Responsibility</p>	<p>The Board shall establish a list of materials, in addition to those stated in law, that are inappropriate for access by minors.</p> <p>The district shall make every effort to ensure that this resource is used responsibly by students and staff.</p> <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 every other user in the district and on the Internet.</p> <p>The building administrator shall have the authority to determine what is inappropriate use.</p>
<p>P.L. 106-554 Sec. 1711, 1721</p> <p>4. Guidelines</p>	<p>The Superintendent or designee shall be responsible for implementing technology and procedures to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to:</p> <ol style="list-style-type: none"> 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. <p>In certain circumstances and with administrative approval, the filtering software may be disabled to allow for bona fide research or other lawful use by district staff members.</p> <p>Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.</p>

Prohibitions

Certain uses of the technology resources, including the Internet, of the district are contrary to the educational mission of the district. Some uses may also constitute a safety hazard to the well-being of students and staff. Therefore, the following activities are strictly prohibited by the district:

1. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Non-work or non-school related work.
4. Product advertisement or political lobbying.
5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
6. Unauthorized or illegal installation, downloading, distribution, reproduction, or use of copyrighted materials or software.
7. Access to obscene or pornographic material or child pornography, including downloading, viewing and printing material that is obscene, pornographic, racist or restricted.
8. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
9. Inappropriate language or profanity.
10. Transmission of material likely to be offensive or objectionable to recipients.
11. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
12. Impersonation of another user, anonymity, and pseudonyms.
13. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
14. Loading or using of unauthorized games (including MUDs), programs, files, or other electronic media.

15. Disruption of the work of other users.
16. Destruction, modification, abuse or unauthorized access to network hardware, software and files.
17. Quoting of personal communications in a public forum without the original author's prior consent.
18. Sharing and/or using others' ID numbers and passwords.
19. Breaking into or attempting to break into other computer systems.
20. Destroying another person's data.
21. Creating and/or sending computer viruses.
22. Student communication through e-mail, Instant Messenger, chat rooms, or other web-based communication services.
23. Checking home-based e-mail accounts.
24. Hacking web sites.
25. Bypassing or attempting to bypass the district filtering software.
26. Purchasing materials through online shopping vendors.
27. Utilizing (FTP) File Transport Protocol.
28. Committing acts of academic dishonesty (cheating on tests or projects).
29. Threatening, harassing, or abusing others through computer technology.
30. Other activities that constitute a safety hazard or are contrary to the educational mission of the district.
31. Unauthorized disclosure of personal information of students and staff.

Undertaking any of these activities is strictly prohibited by the district.

Security

Security on any computer system is high priority, especially when the system involves many users.

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another student's or employee's name.
3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Attempts to log in to the system as any other user may result in cancellation of user privileges and/or other disciplinary actions.

Consequences For Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations; and theft of services will be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions shall be consequences for inappropriate use.

Disciplinary consequences for students may include, but not be solely limited to, the following:

1. Detention.
2. In-school suspension.
3. Out-of-school suspension.

<p>P.L. 94-553 Sec. 107 Pol. 814</p>	<ol style="list-style-type: none">4. Loss of computer/technology privileges.5. Police notification.6. Academic grade reduction (for acts of academic dishonesty).7. Financial restitution (for acts that damage district technology resources). <p>Disciplinary consequences for staff may include, but not be solely limited to, the following:</p> <ol style="list-style-type: none">1. Written reprimand.2. Suspension from duties.3. Demotion.4. Termination of employment. <p>Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses.</p> <p><u>Copyright</u></p> <p>The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.</p> <p><u>Safety</u></p> <p>To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall report such immediately to a teacher or administrator. Network users shall not reveal personal information to other users on the network, including chat rooms, e-mail, Internet, etc.</p> <p>Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.</p>
--	--

P.L. 106-554
Sec. 1732

Internet safety measures shall effectively address the following:

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

Parental Permission Form For Student Use

Students must have a parental permission form on file in the appropriate building administration office before they are allowed to utilize the Internet. By authorizing a student's use of the Internet, parents/guardians agree not to hold the district, schools, or school personnel responsible for any material the student accesses or transmits via the school's computer system.

References:

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

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

Enhancing Education Through Technology Act of 2001 – 20 U.S.C. Sec. 6777

Internet Safety – 47 U.S.C. Sec. 254

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

Board Policy – 814