WEST SHORE SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF COMPUTING RESOURCES AND THE INTERNET

ADOPTED: July 18, 1996

REVISED: September 20, 2001

815. ACCEPTABLE USE OF COMPUTING RESOURCES AND THE INTERNET

1. Purpose

Philosophy

The Board supports the use of the Internet and other computer networks in the District's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration.

For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the School District as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

Pol. 218, 317, 417, 517

The Board also recognizes, however, the potential for misuse of these resources by students, faculty, and staff. Use of these resources by students, faculty, and staff is considered a privilege which may be denied for inappropriate and/or illegal uses as set forth in this and related policies. Furthermore, violations of the guidelines set forth in this policy or other improper use of these resources may result in disciplinary action in accordance with established disciplinary procedures. Such procedures include but are not limited to possible suspension or expulsion for students, suspension for staff and imposition of the penalties under the PA School Code, including but not limited to termination. Appropriate uses of these resources include instruction, independent study, authorized research, and the official work of the offices, departments, recognized student organizations, and agencies of the District.

2. Authority

The electronic information available to students and staff does not imply endorsement by the District of the content, nor does the District guarantee the accuracy of information received. The District is not be responsible for any information that may be lost, damaged or unavailable when using the network or for any information that is retrieved via the Internet.

The District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

	The District reserves the right to monitor, log, control and restrict in size or content, network use, email, and space residing on District workstations or servers, respecting the privacy rights of both District and outside users.
P.L. 106-554 Sec. 1732	The Board establishes that the following materials, in addition to those stated in the law, are inappropriate for access by students and staff: sexually oriented web sites, chat rooms, bulletin boards, newsgroups, or email exchanges; texts, pictures or sounds that are sexually oriented, considered obscene by accepted local standards, and are pornographic or extremely violent.
3. Delegation of Responsibility	The District shall make every effort to ensure that student and staff use these resources responsibly and appropriately in compliance with federal and state law. 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. Students and staff have the responsibility to respect and protect the rights of every other user in the District and on the Internet provided the use is appropriate. The building administrator, in conjunction with Technology and Media Services staff, shall have the authority to determine what is inappropriate use.
P.L. 106-554 Sec 1711, 1721	The Superintendent or designee shall be responsible for developing and using 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: 1. Utilizing a technology protection measure that blocks or filters Internet access for minors and adults to certain visual depictions that are obscene, pornographic, harmful to minors when used by minors, or determined inappropriate by the Board for use by minors. 2. Maintaining and securing a usage log. 3. Monitoring online activities of minors.
4. Guidelines	Network accounts shall be used only by the authorized owner of the account and only for its approved purpose. Network users shall respect the privacy of other users on the system. Exceptions to this guideline will be made where there is reasonable

suspicion of inappropriate use. In that event, an investigation shall be conducted by Technology and Media Services staff or the Superintendent's designee. Examples of inappropriate use are contained in the Prohibitions section which follows. Said examples are not intended to be inclusive.

Prohibitions

Students and staff are expected to act in a responsible, ethical and legal manner in accordance with District policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Illegal activity.
2. Commercial or for-profit purpose.
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, distribution, reproduction, or use of copyrighted materials.
7. Access to obscene or pornographic material or child pornography.
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, 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. Access to sexually oriented chat rooms, e-mail exchanges and/or visuals, texts and sounds that are sexually oriented, obscene, pornographic and extremely violent.

Security

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.

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 violation; 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, including but not limited to suspensions, expulsions and/or termination of employment shall be consequences for inappropriate use. Inappropriate use shall be

	defined as including but not limited to the items contained in the Prohibitions section above. Vandalism will result in cancellation of access privileges. Vandalism is defined as any malicious attempt to harm or destroy equipment, data of another user, Internet or other networks; this includes but is not limited to uploading or creating computer viruses. Vandalism may also result in the filing of criminal charges, suspension or expulsion from school or termination of employment. <u>Copyright</u>
P.L. 94-553 Sec. 107 Pol. 814	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. <u>Safety</u> 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. District computers/servers utilized by students and staff shall be equipped with Internet blocking/filtering software.
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.