

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF INTERNET, COMPUTER, AND NETWORK RESOURCES

ADOPTED: July 18, 1996

REVISED: June 16, 2011

WEST SHORE SCHOOL DISTRICT

<p>1. Purpose</p> <p>Pol. 218, 317, 417, 517</p>	<p>815. ACCEPTABLE USE OF INTERNET, COMPUTER, AND NETWORK RESOURCES</p> <p><u>Philosophy</u></p> <p>The Board supports the use of the Internet, computer, and network resources 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.</p> <p>The District provides students, staff and other authorized individuals with access to the district’s computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.</p> <p>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.</p> <p>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 of employment. 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.</p>
--	--

<p>2. Authority</p> <p>Pol. 218, 233, 317</p> <p>47 U.S.C. Sec. 254</p> <p>Pol. 103, 104, 218.2, 248, 249, 348, 448, 548</p>	<p>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 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.</p> <p>The District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.</p> <p>The Board declares that computer and network use is a privilege, not a right. The District's computer and network resources are the property of the District. Users shall have no expectation of privacy in anything they create, store, send, receive or display on or over the district's Internet, computer, or network resources, including personal files or any use of the district's internet, computer, or network resources. The District reserves the right to monitor, track, and log network access and use; monitor file server space utilization by district users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The District shall cooperate to the extent legally required with the ISP, local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computer, and network resources.</p> <p>The Board requires all users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.</p> <p>The Board establishes that the following materials, in addition to those stated in the law, are inappropriate for access by students and staff: Defamatory, lewd, vulgar, profane, threatening, harassing, discriminatory, bullying, terroristic in nature, or otherwise causes or has the potential to cause a substantial disruption to the operations of the District, the school environment, or the health, safety, or welfare of District students, staff, or visitors.</p>
<p>3. Definitions</p> <p>18 U.S.C. Sec. 2256</p>	<p>The term child pornography is defined under both federal and state law.</p> <p>Child pornography - under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:</p> <ol style="list-style-type: none"> 1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

<p>18 Pa. C.S.A. Sec. 6312</p>	<ol style="list-style-type: none">2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. <p>Child pornography - under state law, is any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act.</p> <p>Federal and state law defines a minor as an individual under the age of eighteen (18) years.</p> <p>The term harmful to minors is defined under both federal and state law.</p>
<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>Harmful to minors - under federal law, is any picture, image, graphic image file or other visual depiction that:</p> <ol style="list-style-type: none">1. Taken as a whole, 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 lewd exhibition of the genitals; and3. Taken as a whole lacks serious literary, artistic, political or scientific value as to minors.
<p>18 Pa. C.S.A. Sec. 5903</p>	<p>Harmful to minors - under state law, is any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:</p> <ol style="list-style-type: none">1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.

<p>18 Pa. C.S.A. Sec. 5903</p>	<p>Obscene - 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 described in the law to be obscene; and 3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational or scientific value.
<p>47 U.S.C. Sec. 254</p> <p>4. Delegation of Responsibility</p>	<p>Technology protection measure - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors.</p> <p>The District shall make every effort to ensure that students and staff use these resources responsibly and appropriately in compliance with federal and state law.</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 provided the use is appropriate.</p> <p>The building administrator, in conjunction with the Assistant Superintendent, shall have the authority to determine inappropriate use. Inappropriate use may include, but is not limited to illegal activity, violation of board policies, accessing, posting, or transmitting profane, obscene, lewd, or pornographic materials, any form of vandalism, hacking network resources, unauthorized access to network accounts, installation of unapproved applications, or bypassing district safety and filtering resources.</p>
<p>P.L. 106-554 Sec 1711, 1721 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>The Superintendent or designee shall be responsible for developing and using technology to determine whether the District's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The practices used shall include but not be limited to:</p>

<p>47 CFR Sec. 54.520</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, 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.
<p>47 U.S.C. Sec. 254</p>	<p>The District shall develop and implement curriculum that ensures students are educated on network etiquette and other appropriate online behavior, including:</p> <ol style="list-style-type: none"> 1. Interaction with other individuals on social networking web sites and in chat rooms.
<p>SC 1303.1-A Pol. 249</p>	<ol style="list-style-type: none"> 2. Cyberbullying awareness and response.
<p>5. Guidelines</p>	<p>Network accounts and Network Credentials shall be used only by the authorized owner of the accounts and only for their approved purposes. 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.</p> <p><u>Prohibitions</u></p> <p>Users 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:</p> <ol style="list-style-type: none"> 1. Illegal activity. 2. Commercial or for-profit purpose. 3. Non-work or non-school related work that does not directly impact or enhance a staff member’s or student’s proficiency with technology and meet an educational purpose for their position or learning in the West Shore School District. 4. Product advertisement or political lobbying.

<p>SC 1303.1-A Pol. 249</p> <p>Pol. 237</p>	<ol style="list-style-type: none">5. Bullying/Cyberbullying.6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.8. Accessing, sending, receiving, transferring, viewing, sharing, or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs, including child pornography.9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.10. Inappropriate language or profanity.11. Transmission of material likely to be offensive or objectionable to recipients.12. Intentional obtaining or modifying of files, passwords, and data belonging to other users.13. Impersonation of another user, anonymity, and pseudonyms.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.19. Accessing the Internet, district computers or other network resources without authorization.
---	---

20. Disabling or bypassing the Internet blocking/filtering software without authorization.

21. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.

22. Use of unapproved personal computing or storage devices on the West Shore School District Network.

23. Use of Web-based Proxies and/or Anonymizers.

Social Media Applications

Online communication is critical to students' learning of 21st Century Skills. The use of Social Media Tools and interactive, online applications offer an authentic, real-world opportunity for student learning. Expectations for classroom blogs, wikis, student protected e-mail, podcast projects, or other Web interactive use shall meet the following guidelines:

1. The use of blogs, podcasts, wikis, or other Social Media Applications are considered an extension of the classroom and student learning. Speech that is prohibited in the classroom is also prohibited in all uses of blogs, podcasts, wikis, or other Social Media Applications.
2. Users are expected to utilize safe practices while using blogs, podcasts, wikis, or other Social Media Applications by not posting unapproved personal information on the web including but not limited to last names, personal details, addresses, phone numbers, or personal photographs.
3. All use of blogs, podcasts, wikis, or other Social Media Applications must be approved by the building principal. Approved uses shall be supervised and be under the direction of a district staff member.

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 Network Credentials / passwords to another individual.

<p>Pol. 237</p>	<ol style="list-style-type: none"> 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. 4. Users who have been approved to connect personal equipment to the West Shore School District Network shall follow all guidelines and procedures as outlined in West Shore School District Board Policy # 237. <p><u>Consequences For Inappropriate Use</u></p>
<p>24 P.S. Sec. 4604</p>	<p>The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.</p> <p>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.</p> <p>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.</p> <p>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.</p>
<p>Pol. 218, 233, 317, 417, 517</p>	<p>Failure to comply with this policy or inappropriate use of the Internet, West Shore School District computer or network resources, shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.</p> <p><u>Copyright</u></p>
<p>P.L. 94-553 Sec. 107 17 U.S.C. Sec. 101 et seq Pol. 814</p>	<p>The illegal use of copyrighted materials and software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.</p>

<p>P.L. 106-554 Sec. 1732 47 U.S.C. Sec. 254 47 CFR Sec. 54.520</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 electronic communication. Any network user who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site 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, social networking web sites, etc.</p> <p>District computers/servers utilized by students and staff shall be equipped with Internet blocking/filtering software.</p> <p>Internet safety measures shall address the following:</p> <ol style="list-style-type: none">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.6. Secure storage of student–created digital files, images, and videos. <p>References:</p> <p>School Code – 24 P.S. Sec. 1303.1-A</p> <p>PA Crimes Code – 18 Pa. C.S.A. Sec. 5903, 6312</p> <p>Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.</p> <p>U.S. Copyright Law – 17 U.S.C. Sec. 101 et seq.</p>
---	--

	<p>Sexual Exploitation and Other Abuse of Children – 18 U.S.C. Sec. 2256</p> <p>Enhancing Education Through Technology Act – 20 U.S.C. Sec. 6777</p> <p>Internet Safety, Children’s Internet Protection Act – 47 U.S.C. Sec. 254</p> <p>Children’s Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520</p> <p>Board Policy – 103, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 417, 448, 517, 548, 814</p>
--	--