



<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>The term harmful to minors is defined under both federal and state law.</p> <p><b><u>Harmful to minors</u></b> – under federal law, is any picture, image, graphic image file, or other visual depiction that:</p> <ol style="list-style-type: none"> <li>1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;</li> <li>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; and</li> <li>3. Taken as a whole lacks serious literary, artistic, political, or scientific value as to minors.</li> </ol>
<p>18 Pa. C.S.A. Sec. 5903</p>	<p><b><u>Harmful to minors</u></b> – 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"> <li>1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;</li> <li>2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and</li> <li>3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.</li> </ol>
<p>18 Pa. C.S.A. Sec. 5903</p>	<p><b><u>Obscene</u></b> – any material or performance, if:</p> <ol style="list-style-type: none"> <li>1. The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest;</li> <li>2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and</li> <li>3. The subject matter, taken as a whole, lacks serious literary, artistic, political, educational, or scientific value.</li> </ol>
<p>47 U.S.C. Sec. 254</p>	<p><b><u>Technology protection measure</u></b> – a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography, or harmful to minors.</p>
<p>3. Authority</p>	<p>The availability of access to electronic information does not imply endorsement by the district of the content, nor does the district guarantee the accuracy of information</p>



<p>24 P.S. Sec. 4604</p>	<p>Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.</p>
<p>24 P.S. Sec. 4610 20 U.S.C. Sec. 6777</p>	<p>Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes. Written permission from the parent/guardian is required prior to disabling Internet blocking/filtering software for a student's use. If a request for temporary disabling of Internet blocking/filtering software is denied, the requesting student or staff member may appeal the denial to the Superintendent or designee for expedited review.</p>
<p>4. Delegation of Responsibility</p>	<p>The district shall make every effort to ensure that this resource is used responsibly by students and staff.</p>
<p>24 P.S. Sec. 4604</p>	<p>The district shall inform staff, students, parents/guardians, and other users about this policy through employee and student handbooks, posting on the district website, and by other appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.</p>
	<p>Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign user agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.</p>
	<p>Student user agreements shall also be signed by a parent/guardian.</p>
	<p>Administrators, teachers, and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discern 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, staff, and other authorized individuals have the responsibility to respect and protect the rights of every other user in the district and on the Internet.</p>
	<p>Building administrators shall make initial determinations of whether inappropriate use has occurred.</p>
<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:</p>

<p>47 CFR Sec. 54.520</p>	<ol style="list-style-type: none"> <li>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 use by minors by the Board.</li> <li>2. Maintaining and securing a usage log.</li> <li>3. Monitoring on-line activities of minors.</li> </ol>
<p>47 U.S.C. Sec. 254</p>	<p>The superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate on-line behavior, including:</p> <ol style="list-style-type: none"> <li>1. Interaction with other individuals on social networking websites and in chat rooms.</li> </ol>
<p>SC 1303.1-A Pol. 249</p>	<ol style="list-style-type: none"> <li>2. Cyberbullying awareness and response.</li> </ol>
<p>5. Guidelines</p>	<p>Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network users shall respect the privacy of other users on the system.</p> <p><b><u>Safety</u></b> It is the district’s goal to protect users of the network from harassment and unwanted or unsolicited electronic communications. 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, social networking websites, etc.</p>
<p>47 U.S.C. Sec. 254 47 CFR Sec. 54.520</p>	<p>Internet safety measures shall effectively address the following:</p> <ol style="list-style-type: none"> <li>1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.</li> <li>2. Safety and security of minors when using electronic mail, chat rooms, and other forms of district electronic communications.</li> <li>3. Prevention of unauthorized on-line access by minors, including “hacking” and other unlawful activities.</li> <li>4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.</li> </ol>

<p>SC 1303.1-A Pol. 249</p> <p>Pol. 237</p> <p>Pol. 814</p>	<p>5. Restriction of minors’ access to materials harmful to them.</p> <p><b><u>Prohibitions</u></b> 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"> <li>1. Facilitating illegal activity.</li> <li>2. Commercial or for-profit purposes.</li> <li>3. Non-work or non-school related work.</li> <li>4. Product advertisement or political lobbying.</li> <li>5. Bullying / Cyberbullying.</li> <li>6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.</li> <li>7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.</li> <li>8. Accessing, sending, receiving, transferring, viewing, sharing, or downloading obscene, pornographic, lewd, or otherwise illegal materials, images, or photographs.</li> <li>9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.</li> <li>10. Inappropriate language or profanity.</li> <li>11. Transmission of material likely to be offensive or objectionable to recipients.</li> <li>12. Intentional obtaining or modifying of files, passwords, and data belonging to other users.</li> <li>13. Impersonation of another user, anonymity, and pseudonyms.</li> <li>14. Fraudulent copying, communications, or modification of materials in violation of copyright laws.</li> <li>15. Loading or using of unauthorized games, programs, files, or other electronic media.</li> </ol>
---	---

<p>17 U.S.C. Sec. 101 et seq Pol. 814</p> <p>24 P.S. Sec. 4604</p>	<p>16. Disruption of the work of others.</p> <p>17. Destruction, modification, abuse or unauthorized access to network hardware, software, and files.</p> <p>18. Accessing the Internet, district computers, or other network resources without authorization.</p> <p>19. Disabling or bypassing the Internet blocking/filtering software without authorization.</p> <p>20. Accessing, sending, receiving, transferring, viewing, sharing, or downloading confidential information without authorization.</p> <p><b><u>Security</u></b> 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, these guidelines shall be followed:</p> <ol style="list-style-type: none"><li>1. Employees and students shall not reveal their passwords to another individual.</li><li>2. Users are not to use a computer that has been logged in under another student's or employee's name.</li><li>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.</li></ol> <p><b><u>Copyright</u></b> The illegal use of copyrighted materials 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><b><u>District Website</u></b> The district may establish and maintain a website and shall develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All users publishing content on the district web site shall comply with this and other applicable district policies.</p> <p>Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the building principal.</p> <p><b><u>Consequences for Inappropriate Use</u></b> The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.</p>
--	---

<p>Pol. 218, 233, 317</p>	<p>Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall 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.</p> <p>Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings. 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>Failure to comply with this policy or inappropriate use of the Internet, district network or computers shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.</p> <p><b><u>References:</u></b>          School Code – 24 P.S. Sec. 1303.1-A          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.          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, Children’s Internet Protection Act – 47 U.S.C. Sec. 254          Children’s Internet Protection Act Certifications, Title 47, Code of Federal Regulations – 47 CFR Sec. 54.520          Board Policy – 103, 103.1, 104, 218, 218.2, 220, 233, 237, 248, 249, 317, 348, 814</p>
---------------------------	--