

<p>18 Pa. C.S.A. Sec. 6312</p>	<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>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; and 3. 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; and 3. 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>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>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 received. The district shall 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.</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>Pol. 218, 233, 317</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. Use of the system is governed by this policy. Users shall have no expectation of privacy in anything they create, store, send, receive or display on or over the district's Internet, computers or network resources, including personal files or any use of the district's Internet, computers or network resources. The district reserves the right to monitor, track, and log network access and use; monitor filespace 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 Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's Internet, computers 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>47 U.S.C. Sec. 254</p>	<p>The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors:</p> <ol style="list-style-type: none"> 1. Defamatory. 2. Lewd. 3. Vulgar. 4. Profane. 5. Threatening.

<p>Pol. 103, 104, 248, 348</p>	<p>6. Harassing.</p>
<p>Pol. 103, 104, 248, 348</p>	<p>7. Discriminatory.</p>
<p>Pol. 249</p>	<p>8. Bullying.</p>
<p>Pol. 218.2</p>	<p>9. Terroristic.</p>
<p>24 P.S. Sec. 4604 20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254</p>	<p>The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.</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 web site, 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.</p>

<p>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec. 54.520</p> <p>47 U.S.C. Sec. 254</p> <p>SC 1303.1-A Pol. 249</p>	<p>Student user agreements shall also be signed by a parent/guardian.</p> <p>Parents/Guardians have the right to request the termination of their child’s account.</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>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> <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>The Superintendent or designee shall develop and implement administrative regulations that ensure 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. 2. Cyberbullying awareness and response.
--	---

- b. Users will not agree to meet with someone they have met online without their parent's/guardian's approval and participation.
- c. Users will promptly disclose to their teachers or other school employees any message they receive that is inappropriate or makes them feel uncomfortable.
- d. Student photographs:
 - 1) K-6: Parents/Guardians may notify the building principal if they object to the publishing of individual or group photographs where their student is not identified. If schools wish to publish photos with student identification, written parent/guardian permission is required.
 - 2) Parents/Guardians may notify the building principal if they do not wish to have photos of their students published, whether or not the student can be identified.

E-mail

- 1. Individual E-mail Accounts For Students. Students will not be provided with individual e-mail accounts. Students may not access any type of e-mail including, but not limited to, web-mail and POP accounts during school hours unless monitored by a staff member.
- 2. Individual E-mail Accounts For District Employees. Permanent full-time district employees may be provided with an individual account. E-mail is the property of the district and employees should have no reasonable expectation of privacy when using district e-mail.
- 3. Users will not post chain letters or engage in "spamming". Spamming is sending an annoying or unnecessary message to a large number of people.
- 4. Users with district supplied e-mail will check their e-mail frequently, delete unwanted messages promptly, and stay within their e-mail quota.
- 5. Users will subscribe only to high quality discussion group mail lists that are relevant to their educational or professional/career development.

<p>SC 1303.1-A Pol. 249</p>	<p><u>Inappropriate Material</u></p> <p>If a user inadvertently accesses material that is profane or obscene (pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature), they should immediately disclose the inadvertent access to the supervising adult or building principal. This will protect users against an allegation that they have intentionally violated the Acceptable Use Policy.</p> <p><u>Selection Of Material</u></p> <p>When using the Internet for class activities, teachers will make every effort to select material that is age appropriate and that is relevant to the course objectives. Teachers will preview the materials and sites they require or recommend students to access, in order to determine the appropriateness of the material contained on or accessed through the site. District employees may access the above material only in the context of legitimate research.</p> <p>Teachers will make an effort to provide guidelines and lists of resources to assist their students in channeling their research activities effectively and properly. Teachers will assist their students in developing the skills to ascertain the truthfulness of information, distinguish fact from opinion, and engage in discussions about controversial issues while demonstrating tolerance and respect for those who hold divergent views.</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. Commercial or for-profit purposes.2. Nonwork or nonschool related work.3. Product advertisement or political lobbying.4. Bullying/Cyberbullying.5. Hate mail, discriminatory remarks, and offensive or inflammatory communication.6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
---------------------------------	--

815.1. ACCEPTABLE USE OF INTERNET, COMPUTERS AND NETWORK RESOURCES - Pg. 9

<p>Pol. 237</p>	<p>7. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.</p> <p>8. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.</p> <p>9. Inappropriate language or profanity.</p> <p>10. Transmission of material likely to be offensive, objectionable, or threatening to recipients.</p> <p>11. Intentional obtaining, modifying, and transferring of files, passwords, codes, and data belonging to other users without authorization.</p> <p>12. Impersonation of another user, account, anonymity, and pseudonyms.</p>
<p>Pol. 814</p>	<p>13. Fraudulent copying, communications, or modification of materials in violation of copyright laws.</p> <p>14. Installation, use, or duplication of unauthorized games, programs, files, or other electronic media.</p> <p>15. Disruption of the work of other users.</p> <p>16. Destruction, modification, abuse, theft, or unauthorized access to network hardware, software and files.</p> <p>17. Accessing the Internet, district computers or other network resources without authorization.</p> <p>18. Disabling or bypassing the Internet blocking/filtering software without authorization. The district uses filtering software in an attempt to limit access to inappropriate world web sites. The district does not guarantee that such software will prevent user access to all inappropriate or objectionable material. Parents/Guardians are responsible to discuss with their child what is considered appropriate and inappropriate based on their own family values.</p> <p>19. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.</p> <p>20. Knowingly or recklessly posting false or defamatory information about a person or organization.</p>

	<p>21. Posting information that, if acted upon, could cause damage or disruption.</p> <p>22. Illegal Activities (United States Code – Title 18, Part I, Chapter 47 [The Computer Fraud and Abuse Act], United States Code – Title 18, Part I, Chapter 121 [Stored Wire and Electronic Communications And Transactional Records Act]).</p> <ul style="list-style-type: none">a. Users will not attempt to gain unauthorized access to the district system or to any other computer system through the district system, or go beyond their authorized access. This includes attempting to log in through another person’s account or access another person’s files.b. Users will not make deliberate attempts to disrupt the computer system or destroy data.c. Users will not use the district system to engage in any other illegal act, such as arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, threatening the safety of person or property, etc. <p>23. Nondisclosure of improper events such as accidentally viewing passwords, accessing inappropriate web sites, etc. to the appropriate authority.</p> <p>24. Attempting to undermine or thwart any computer related rule, procedure, security measure, or common sense courtesy.</p> <p><u>Respecting Network Resources</u></p> <ul style="list-style-type: none">1. Users will use the system only for educational and professional/career development activities and limited individual, personal research.2. Users will not download large files unless absolutely necessary. If necessary, users will download the files at a time when the system is not being heavily used and immediately remove the file from the system computer to their personal computer.
--	--

<p>17 U.S.C. Sec. 101 et seq Pol. 814</p>	<p><u>Security</u></p> <p>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">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. <p><u>Plagiarism</u></p> <p>Users shall not plagiarize works that they find on the Internet. Plagiarism is taking the ideas or writings of others and presenting them as if they were original to the user.</p> <p><u>Copyright</u></p> <p>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. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not they can use a work, they should request permission from the copyright owner.</p> <p><u>District Web Site</u></p> <p>The district shall establish and maintain a web site 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. Teachers are responsible for maintaining their own web pages.</p> <p>Users shall not copy or download information from the district web site and disseminate such information on unauthorized web pages without authorization from the building principal.</p>
---	---

<p>24 P.S. Sec. 4604</p>	<p>With the approval of the building principal, school-sponsored extracurricular organizations may establish web pages. The principal will establish a process and criteria for the establishment and posting of material, including links to other sites, on this page. Materials presented on the organization web page must relate specifically to organization activities and will include only student-produced material. Organization web pages must include the following notice: “This is a school-sponsored student extracurricular organization web page. Opinions expressed on this page shall not be attributed to the district.”</p> <p><u>District Limitation Of Liability</u></p> <p>The district makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the district system will be error-free or without defect. The district will not be responsible for any damage users may suffer including, but not limited to, loss of data or interruptions of service. The district is not responsible for the accuracy or quality of the information obtained through or stored on the system. The district will not be responsible for financial obligations arising through the unauthorized use of the system.</p> <p><u>Search And Seizures</u></p> <ol style="list-style-type: none"> 1. System users should have no reasonable expectation of privacy of their data and e-mails. 2. Routine maintenance and monitoring of the system may lead to discovery that the user has or is violating the district Internet Acceptable Use Policy or the law. 3. An individual search may be conducted if there is reasonable suspicion that a user has violated the law or district policy/procedure. The nature of the investigation will be reasonable and in the context of the nature of the alleged violation. 4. District employees should be aware that their personal files may be accessible under public record laws. <p><u>Consequences For Inappropriate Use</u></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 or data belonging to others; copyright violations; and theft of services shall be reported to the appropriate legal authorities for possible prosecution.</p>
------------------------------	--

<p>Pol. 218, 233, 317</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>Disciplinary actions will be tailored to meet specific concerns related to the violation and to assist the student in gaining the self-discipline necessary to behave appropriately on an electronic network.</p> <p>Employee violations of the district Internet Acceptable Use Policy will be handled in accordance with the district disciplinary procedures.</p> <p>The district will cooperate fully with local, state, or federal officials in any investigation concerning or relating to any illegal activities conducted through the district system.</p> <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, 814</p>
--	---