

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, 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.

<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, the following 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>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 of data belonging to others; copyright violations; 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 shall be consequences for inappropriate use.</p> <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>47 U.S.C. Sec. 254</p> <p>17 U.S.C. Sec. 101 et seq</p> <p>20 U.S.C. Sec. 6777</p> <p>47 U.S.C. Sec. 254</p> <p>PA Code Title 22 Sec. 403.1</p> <p>Board Policy 814</p>	<p>Any district computer/server utilized by students and staff shall be equipped with Internet blocking/filtering software.</p> <p>Internet safety measures shall effectively 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.
--	---