

SECTION: OPERATIONS

TITLE: INTERNET SAFETY AND USE

ADOPTED: July 22, 2002

REVISED: February 28, 2005

# FAIRVIEW SCHOOL DISTRICT

	<p style="text-align: center;">815.2. INTERNET SAFETY AND USE</p> <p><u>Overview</u></p> <p>Technology resources are available via the Internet and the local area network in the Fairview School District. We are pleased to provide this access in our schools and believe these resources offer vast, diverse, and unique opportunities to both students and staff. Our goal in providing this service to students and staff is to provide educational excellence in the Fairview community by facilitating resource sharing, innovation, and communication. Students and staff are responsible for appropriate behavior on computer networks. With access to these technology resources comes the availability of material that may <u>not</u> be considered of educational value in the context of the school setting. Despite the availability of filters and blocking software, students and staff might nevertheless gain access to electronic information that may not be appropriate. In such cases, general school rules for behavior and communications apply.</p> <p>Students and staff are expected to use the Internet and FSD hardware as educational resources. The Fairview School 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. The Fairview School District will not be responsible for any unauthorized charges or fees resulting from access to the Internet. The following procedures and guidelines are used to help ensure appropriate use of technology resources, including the Internet, in the Fairview School District. All FSD resources must be used appropriately. This Internet Safety and Use Policy (ISUP) addresses the following requirements set by the Federal Communications Commission (FCC):</p> <ol style="list-style-type: none"> <li>1. Access by minors to inappropriate matter on the Internet and World Wide Web.</li> <li>2. The safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communication.</li> <li>3. Unauthorized access, including so-called “hacking” and other unlawful activities by minors online.</li> </ol>
--	--

<p>P.L. 106-554 Sec. 1711, 1721 SC 4601 et seq</p>	<ol style="list-style-type: none"> <li>4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.</li> <li>5. Measures designed to restrict minors' access to materials harmful to minors.</li> <li>6. Monitoring the online activities of minors.</li> </ol> <p>The policy of Internet safety must include a technology protection measure that protects against Internet access by both adults and minors to visual or written depictions that are obscene or child pornography, or, with respect to use of the computers by minors, harmful to minors.</p>
<p>P.L. 106-554 Sec. 1711, 1721 SC 4601 et seq</p>	<p>Prohibitions of technology and Internet use include but are not limited to the following:</p> <ol style="list-style-type: none"> <li>1. Technology users shall not access inappropriate material on the Internet or World Wide Web, including but not limited to: hate mail, discriminatory remarks, and/or offensive or inflammatory communication.</li> </ol>
<p>SC 4601 et seq</p>	<p>Technology users shall not use computer equipment or communication services owned or leased by the district for sending, receiving, viewing or downloading written or visual depictions of pornography, obscenity, child pornography, or other materials that may be "harmful to minors."</p>
<p>SC 4601 et seq</p>	<p>The Fairview School District currently uses the N2H2 filtering software to limit access to unacceptable web sites. This is through participation in the filtering program utilized by the Northwest Tri-County Intermediate Unit. The N2H2 filtering software is provided by N2H2, Inc. The district finds that the N2H2 filtering software restricts access to web sites which are inappropriate to be accessed in a school environment. Access to such web sites would not be in accordance with the district's curriculum and policies. The Fairview School District has, thus, determined that the filtering category definitions provided by N2H2, Inc. establish the proper criteria for determination of inappropriateness of web sites for minor children and students within the district. The district has appended hereto the filtering category definitions, including the introductory paragraphs and special rules, from N2H2, Inc.</p> <ol style="list-style-type: none"> <li>2. Technology users shall not use chat rooms or other forms of direct electronic communication such as newsgroups, streaming video (tickers), etc. for non-educational purposes.</li> </ol>

<p>Pol. 814</p>	<p>3. Technology users shall not engage in unauthorized access of computers, including “hacking,” whether by spyware designed to steal information, or viruses and worms designed to damage computers or strip information, or completely take over a person’s computer.</p> <p>4. Technology users shall not engage in unlawful activities.</p> <p>5. Technology users shall not disclose, use, or disseminate any personal identification information of themselves or others.</p> <p>6. Technology users will not quote personal communications in a public forum without the original author’s prior consent.</p>
<p>Pol. 814</p>	<p>7. Unauthorized or illegal installation, distribution, reproduction, modification, or use of copyrighted materials is prohibited, as specified in FSD Copyright Policy.</p> <p>8. Technology users shall not engage in the destruction, modification, or abuse of FSD technology resources including but not limited to hardware and/or software.</p>
<p>SC 4601 et seq</p>	<p>9. The illegal installation and/or utilization of copyrighted/unauthorized games, programs, files, or other electronic media on FSD computers is prohibited, as specified in the FSD Copyright Policy.</p> <p>10. Fairview School District retains ownership and rights of access to all files stored on the equipment under the control of the agency.</p> <p>11. FSD technology users shall use technology resources for educational purposes.</p> <p>12. The district’s technology coordinator or his/her designee shall be permitted to disable the software program for an adult, or a minor who provides written consent from a parent/guardian, to enable access for bona fide research or other lawful purpose. The purpose for which the software is to be disabled shall be in writing to the technology coordinator, who shall also be permitted to monitor or log the use of the technology equipment to confirm that the actual use is consistent with the purpose. Nothing in this policy shall be construed to permit any person to have access to material the character of which is illegal under federal or state law.</p> <p><u>Staff Expectations in Use of Technology Resources</u></p> <p>1. Staff members shall use technology resources only for educational purposes.</p>

<p>SC 4601 et seq</p>	<ol style="list-style-type: none"><li>2. Staff members shall not engage in unauthorized access of computers, including “hacking.”</li><li>3. Staff members shall not engage in unlawful activities.</li><li>4. Staff members shall not disclose, use, or disseminate any personal identification information of students.</li><li>5. Staff members shall monitor student use of technology resources.</li><li>6. Staff members shall not disclose their network passwords to anyone, other than a network administrator.</li><li>7. Any use of the network for commercial or for-profit purposes, product advertisement, political lobbying, or illegal activity is prohibited.</li><li>8. Staff members shall not access inappropriate material on the Internet or World Wide Web, including but not limited to: hate mail, discriminatory remarks, and/or offensive or inflammatory communication. Staff members shall not use computer equipment or communication services owned or leased by the district for sending, receiving, viewing or downloading written or visual depictions of pornography, obscenity, child pornography, or other materials that may be “harmful to minors.”</li><li>9. Staff members shall access and review a web site before they refer students to the web site. Staff members shall refer students only to those web sites that are accessible through the district’s filtering software.</li></ol> <p><u>Student Expectations in Use of Technology Resources</u></p> <ol style="list-style-type: none"><li>1. Be courteous and respectful in your communications to others.</li><li>2. Use appropriate language. No swearing, vulgarities, suggestive, obscene, belligerent, or threatening language. Illegal activities are strictly forbidden.</li><li>3. Do not reveal your home address, phone number(s), password(s) or those of other students. Use school addresses and phone numbers only, even if you think you know your correspondent.</li><li>4. Do not disclose your network passwords to anyone.</li></ol>
-----------------------	---

<p>SC 4601 et seq</p>	<ol style="list-style-type: none"> <li>5. Note that electronic mail (e-mail) is not guaranteed to be private. People who operate the system do have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.</li> <li>6. Do not post personal messages on bulletin boards or “listservs.” Send personal messages directly to the person to whom you want to write.</li> <li>7. Users shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent/ impersonate other users on the network.</li> <li>8. Any use of the network for commercial or for-profit purposes, product advertisement, political lobbying, or illegal activity is prohibited.</li> <li>9. Do not use the network in such a way that you disrupt the work of others.</li> <li>10. Students shall not access inappropriate material on the Internet or World Wide Web, including but not limited to: hate mail, discriminatory remarks, and/or offensive or inflammatory communication. Students shall not use computer equipment or communication services owned or leased by the district for sending, receiving, viewing or downloading written or visual depictions of pornography, obscenity, child pornography, or other materials that may be “harmful to minors.”</li> </ol>
<p>P.L. 106-554 Sec. 1711, 1721</p>	<p><u>Enforcement of Policy</u></p> <p>The Fairview School District uses a technology protection measure that blocks or filters access to some World Wide Web sites that are not in accordance with the Fairview School District curriculum and policies. This measure protects against access by adults and minors to visual or written depictions that are obscene, child pornography or – with respect to use of computers with Internet access by minors – harmful to minors. Filtering may be disabled for adults engaged in bona fide research or other lawful purposes. To ensure enforcement of the policy, the Fairview School District will monitor use of technology resources through direct supervision, monitoring Internet use history, or various software and hardware tools. The Fairview School District currently uses the N2H2 filtering software to limit access to unacceptable web sites. (Students do not have access to chat rooms.) The district finds web sites to which access is limited by the N2H2 filtering software, as developed by N2H2, Inc. and utilized by the Northwest Tri-County Intermediate Unit, are inappropriate web sites. Access to such web sites is not in accordance with the district’s curriculum and policies and will be blocked, as set forth in the N2H2 filtering category definitions appended to this policy.</p>



815.2. INTERNET SAFETY AND USE - Pg. 7

PA Code  
Title 22  
Sec. 403.1

Board Policy  
814