

<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>The term harmful to minors is defined under both federal and state law.</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>Technology protection measure - a specific technology that blocks or filters Internet</p>

<p>47 U.S.C. Sec. 254</p>	<p>access to visual depictions that are obscene, child pornography or harmful to minors.</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>3. Authority</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. 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 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>47 U.S.C. Sec. 254</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</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, vulgar, or profane. 3. Threatening.
<p>Pol. 103, 103.1, 104, 248, 348</p>	<ol style="list-style-type: none"> 4. Harassing or discriminatory.
<p>Pol. 249</p>	<ol style="list-style-type: none"> 5. Bullying.
<p>Pol. 218.2</p>	<ol style="list-style-type: none"> 6. Terroristic.

<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>Parents/Guardians who do not want their child to have access to the Internet should put the request in writing to building administrator.</p> <p>Administrators, teachers and staff have a professional responsibility to work together to help students understand proper use of the network, 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 and 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>20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254 47 CFR Sec.54.520</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>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 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. Cyber bullying awareness and response.
<p>SC 1303.1-A Pol. 249</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>5. Guidelines</p> <p>47 U.S.C. Sec. 254 47 CFR Sec. 54.520</p>	<p><u>Safety</u></p> <p>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 web sites, etc.</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.

<p>Pol. 814</p>	<ol style="list-style-type: none">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. Fraudulent copying, communications, or modification of materials in violation of copyright laws.15. Loading or using of unauthorized games, programs, files, or other electronic media.16. Disruption of the work of other users.17. Destruction, modification, abuse or unauthorized access to network hardware, software and files.18. Accessing the Internet, district computers or other network resources without authorization.19. Disabling or bypassing the Internet blocking/filtering software without authorization.20. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization. <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>24 P.S. Sec. 4604</p>	<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. The district shall cooperate fully with local, state or federal officials in any investigation related to any illegal activities conducted through the network.</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. The district reserves the right to temporarily or permanently remove a user account on the network to prevent further unauthorized activity. The district shall make determinations on whether specific uses of the network are consistent with acceptable use.</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>Pol. 218, 233, 317</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>17 U.S.C. Sec. 101 et seq Pol. 814</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.</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.</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>

Google Apps

The district will provide a Google Apps account for students and staff for the purpose of school-related projects. Google Apps provides the opportunity to collaborate and share information electronically. Use of Google Apps shall be in accordance with Board policy, administrative regulations, and Google Apps Terms of Service.

Laptops

Muhlenberg School District seeks to provide an appropriate office desktop computer system for each fulltime faculty and staff member, within budgetary constraints. Full time faculty and staff members may have the option to have a laptop computer instead of a desktop computer.

Laptops will be authorized based upon job responsibilities, demonstrated need, and school/department approvals. All decisions of administration are final.

Ownership of the laptop computer will reside with the Muhlenberg School District. The laptop (including case and packaged items) must be returned to the appropriate building representative upon termination of employment at their assigned school.

The assigned faculty/staff member assumes the responsibility of security and care of the laptop. The faculty/staff members will be responsible for certain costs to repair or replace the computer if the damage or loss is due to negligence or intentional misconduct.

References:

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

	<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, 103.1, 104, 218, 218.2, 220, 226, 233, 237, 248, 249, 317, 348, 814</p>
--	---