Lebanon School District

SECTION: PUPILS

TITLE: Child Pornography

ADOPTED: March 21, 2016

REVISED:

	218.4 Child Pornography
1. Purpose	The Board supports use of the computers, Internet and other network resources in the district's instructional and operational programs in order to facilitate learning, teaching and daily operations through interpersonal communications and access to information, research and collaboration. The district provides students, staff and other authorized individuals with access to the district's computers, electronic communication systems and network, which includes Internet access, whether wired or wireless, or by any other means.
2. Definition 18 U.S.C. Sec. 2256	The term child pornography is defined under both federal and state law. **Child pornography** - under federal law, is any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where: 1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct; 2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or 3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct. **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. The term harmful to minors is defined under both federal and state law. **Harmful to minors** - under federal law, is any picture, image, graphic image file or other visual depiction that: 1. Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion;

18 Pa.C.S.A. Sec. 6312	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. **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:
20 U.S.C. Sec. 6777 47 U.S.C. Sec. 254	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. **Obscene** - any material or performance, if:
18 Pa.C.S.A. Sec. 5903	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. **Technology protection measure** - a specific technology that blocks or filters Internet access to visual depictions that are obscene, child pornography or harmful to minors. 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. The district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or other network resources.
18 Pa.C.S.A Sec 5903	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, delete, 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 fileserver space 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.
47 U.S.C. Sec. 254	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.
	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:
3. Authority	1. Threatening. 2. Harassing or discriminating. 3. Bullying 4. Terroristic
	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.
	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.
	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.
	The district shall make every effort to ensure that this resource is used responsibly by students and staff.
	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.

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

Student user agreements shall also be signed by a parent/guardian.

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.

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.

Building administrators shall make initial determinations of whether inappropriate use has occurred.

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:

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.

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:

1. Interaction with other individuals on social networking websites and in chat rooms.

2. Cyberbullying awareness and response.

4. Delegation of Responsibility	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. <u>Safety</u> 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, email, social networking websites, etc. Internet safety measures shall effectively address the following: 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. <u>Prohibitions</u> Users are expected to act in a responsible, ethical and legal manner in accordance with district policy and procedures, accepted rules of network etiquette, and federal and state law and regulations. Specifically, the following uses are prohibited: 1. Users shall not use the district's Internet, computers or network resources to access, send, receive, transfer, view, share, or download material that is profane, obscene, pornographic, advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature). 2. Students shall not agree to meet with someone they have met on the Internet without their parent's/guardian's approval and participation. 3. Users shall not attempt to gain unauthorized access to any computer system or

	network. This includes attempting to log in through another person's account or access another person's files. These actions are illegal, even if only for the purposes of browsing, snooping, or electronic discovery. 4. Users shall not deliberately disrupt or harm hardware, systems or files; interfere with computer or network performance; interfere with another's ability to use equipment and systems; or destroy data. 5. Users shall not use the district's Internet, computers or network resources to engage in illegal acts, such as arranging for a drug sale or the purchase of alcohol; engaging in criminal gang activity; threatening the safety of persons; and accessing, sharing, distributing or reproducing unauthorized copyrighted materials. 6. Users shall not utilize peer-to-peer file sharing applications or execute programs to facilitate the downloading or exchange of copyrighted or unauthorized materials. 7. Users shall not use the district's Internet, computers or network resources to solicit information with the intent of using such information to cause personal harm or bodily injury to another or others. 8. Users shall not post or distribute information that could endanger an individual, cause personal damage or cause service disruption. 9. Users shall not knowingly or recklessly post false or defamatory information about a person or organization.
5. Guidelines	10. Users shall not intentionally seek information on, obtain copies of, or modify files, data or passwords belonging to other users. 11. Users shall not indirectly or directly make network connections that create backdoors to the district, other organizations, community groups, etc., that allow unauthorized access to the district's network. 12. Users shall not use obscene, profane, lewd, vulgar, rude, inflammatory, hateful, threatening or disrespectful language. 13. Users shall not engage in personal attacks, including prejudicial or discriminatory attacks. 14. Users shall not harass another person. 15. Users shall not repost or distribute a message that was sent to them privately without the permission of the person who sent the message.

16. Users shall not forward or post chain letters or engage in spamming. Spamming is sending an annoying or unnecessary message to a large number of people.

17. Users shall not install, use or reproduce unauthorized or unlicensed software on district resources.

18. Users shall not plagiarize works that they find on the Internet or other resources.

19. Users shall not use district Internet, computers, or network resources for private business activities, commercial or for-profit purposes, product advertisement, or unreasonable personal use.

20. Users shall not use the district's Internet, computers, or network resources for political lobbying.

21. Students shall not download files unless approved by their teacher.

22. Users shall not engage in bullying/cyberbullying.

23. Students shall not access material that is harmful to minors or is determined inappropriate for minors in accordance with school policy.

24. Users shall not transmit material likely to be offensive or objectionable to recipients.

25. Users shall not engage in impersonation of another user, anonymity, and pseudonyms.

26. Users shall not disable or bypass the Internet blocking/filtering software without authorization. This includes, but is not limited to, the use of proxy avoidance type software and hardware as well as filesharing software.

27. Users shall not access, send, receive, transfer, view, share or download confidential information without authorization.

28. Users are prohibited from directly registering or obtaining Internet domain names, Internet address space, security certificates or other related Internet services on behalf of or representing any school, administrative office or the district as a whole.

29. Users may not acquire, contract with, or utilize unauthorized technology-based software, hardware or external hosting services on behalf of or representing

any school, administrative office or the district as a whole.

Security

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:

1. Users 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. Every account shall be limited to one (1) active session at a time.

4. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

5. Unauthorized attempts to log on to the district's network or any other network as a system administrator is prohibited.

6. Users should immediately notify a teacher or system administrator of any possible security problem.

Copyright

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.

Consequences For Inappropriate Use

Users shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

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.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy.

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. 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, in accordance with applicable law, regulations and LSD policies.