WEST ALLEGHENY SCHOOL DISTRICT

SECTION: 815

TITLE: Acceptable Use of Internet, Computers and Network Resources

ADOPTED: 2002

REVISED: 2013, 2022

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. Internet users are expected to access the Internet and World Wide Web as an educational resource. The Internet and World Wide Web are available in the district as a resource to promote and enhance the educational experience. All District technology resources including the Internet, World Wide Web resources, and approved personal electronic devices for student use must be used appropriately and explicitly for educational purposes only. For instructional purposes, the use of network facilities shall be consistent with the curriculum adopted by the district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students. **The school district will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.** As a public school entity receiving federal funds, this policy is also required for purposes of complying with the Child Internet Protections Act (CIPA) and regulations adopted by the Federal Communications Commission (FCC). Signed user agreements pursuant to this policy shall be executed by students, parents and staff electronically.
Definitions	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;

	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 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.[2] 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:[3][4] Taken as a whole, with respect to minors, appeals to a prurient interest in nudity, sex or excretion 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 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:[5] Predominantly appeals to the prurient, shameful, or morbid interest of minors; Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable for minors; and Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors. **Obscene** - any material or performance, if:[5] The average person applying contemporary community standards would find that the subject matter taken as a whole appeals to the prurient interest; The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and 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.

Authority	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. 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.[6][7][8] 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:[4] 1. Defamatory. 2. Lewd, vulgar, or profane. 3. Threatening. 4. Harassing or discriminatory.[9][10][11] 5. Bullying.[12] 6. Terroristic.[13] 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.[3][4][14] 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.[14] 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.[3][15] Your rights to free speech, as set forth in the Student Rights and Responsibilities Policy (SRRP) and the Code of Student Conduct, apply also to your communication on the Internet. The West Allegheny School District Internet system is considered a limited forum, similar to the school newspaper, and therefore, the District may restrict your speech for valid educational reasons. The district will not restrict your speech on the basis of a disagreement with the opinions you are expressing. Search and Seizure 1. Routine maintenance and monitoring of the West Allegheny School District Internet system network resources may lead to discovery that you have violated this policy, The SRRP, the School Code of conduct and/or the law. 2. An individual search will be conducted if there is reasonable suspicion that you have violated this Policy, the SRRP, or the law. The investigation will be reasonable and related to the suspected violation. 3. Your parents/guardians have the right at any time to request to see the contents of your e-mail file. Due Process 1. The District will cooperate fully with local, state or federal officials in any investigation related to any illegal activities conducted through the West Allegheny School District technology resources, network or Internet system. 2. In the event there is a claim that you have violated this Policy, the SRRP or the Student Code of conduct in your use of the West Allegheny School District Internet system, you will be provided with notice and opportunity to be heard in the manner set forth in the SRRP. 3. If the violation also involves a violation of other provisions of the SRRP, it will be handled in a manner described in the SRRP. Additional restrictions may be placed on your use of your Internet account.
Delegation of Responsibility	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.[14] 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 { } and tracking systems to track and recover lost or stolen equipment. 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:[3][4][16] 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:[4] 1. Interaction with other individuals on social networking websites and in chat rooms. 2. Cyberbullying awareness and response.[12][17]
Guidelines	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:[4][16] 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.

Prohibitions

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:

1. Facilitating illegal activity.

2. Commercial or for-profit purposes.

3. Nonwork or nonschool related work.

4. Product advertisement or political lobbying.

5. Bullying/Cyberbullying.[12][17]

6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.

7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.[18]

9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.

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.[19]

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.

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. 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.

Network accounts shall be used only by the authorized owner of the account for its approved purpose. All communications and information accessible via the network should be assumed by all users to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.

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.[19][20]

District Website

The district may

establish and maintain a website 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 website shall comply with this and other applicable district policies.

Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the building principal.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[14]

	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.[6][7][8]

NOTES:
State CIPA – Child Internet Protection Act – 24 P.S. Sec. 4601 et seq.
Federal CIPA – Children's Internet Protection Act – 47 U.S.C. Sec. 254
PSBA Revision 11/10 © 2019 PSBA

Legal
1. 18 U.S.C. 2256
2. 18 Pa. C.S.A. 6312
3. 20 U.S.C. 7131
4. 47 U.S.C. 254
5. 18 Pa. C.S.A. 5903
6. Pol. 218
7. Pol. 233
8. Pol. 317
9. Pol. 103
10. Pol. 103.1
11. Pol. 104
12. Pol. 249
13. Pol. 218.2
14. 24 P.S. 4604
15. 24 P.S. 4610
16. 47 CFR 54.520
17. 24 P.S. 1303.1-A
18. Pol. 237
19. Pol. 814
20. 17 U.S.C. 101 et seq
18 Pa. C.S.A. 2709
24 P.S. 4601 et seq
Pol. 220
School Code - 24 P.S. §510, 1303, 1317.1
Federal Wiretapping and Electronic Surveillance Act - 18 U.S.C. Sec. 2510
Pennsylvania Wiretapping and Electronic Surveillance Act - 18 Pa. C.S.A. Sec. 5703
Internet Safety - 47 U.S.C. Sec. 254
Child Internet Protection Act - 24 P.S. Sec. 4601
Federal Communications Commission regulations