TECHNOLOGY ACCEPTABLE USE POLICY 6270

6270 The Board supports use of the Internet and other computer networks in West Allegheny School 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.

Internet users are expected to use the Internet and World Wide Web as an educational resource. The Internet and World Wide Web have been available in the district as a resource to promote and enhance the educational experience. All District Internet and World Wide Web resources 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 each student.

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 and remain on file in the office of each building. Forms are available in all building offices.

6270.1 DISCLAIMER

The electronic information available to students and staff 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 received via the Internet.

The District shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.

6270.2 NO EXPECTATION OF PRIVACY

There is no expectation of privacy for any user of the West Allegheny School District's computer network, including Internet access and e-mail.

Users shall have no expectation of privacy in anything created, stored, sent or received on a District computer.

West Allegheny retains the right, but not the duty, to randomly or specifically monitor without prior notice, any person's use to ensure that the computer network

is being used properly, to ensure that it is used in compliance with CIPA, to prevent waste and misuse, for purposes of maintenance, and/or with reasonable cause to suspect misuse of the computer network. This monitoring includes accessing files and communication.

The District reserves the right to log network use and to monitor fileserver space utilization by District users.

6270.3 PRIVILEGE/NOT A RIGHT

The Board establishes that network use is a privilege, not a right; inappropriate, unauthorized and illegal use may result in cancellation of those privileges and/r appropriate disciplinary action.

6270.4 COMPLIANCE

The Board establishes that any information that is obscene, child pornographic or harmful to minors, all as defined by the Child Internet Protections Act (CIPA), is inappropriate for access by minors.

The Superintendent or his/her designee shall be responsible for implementing technology and procedures to determine whether the District's computers are being used for purposes prohibited by law or this Policy. The procedure shall include, but not be limited to:

a. 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.
b. The Superintendent or designee shall have the authority to determine what inappropriate use is.

6270.5 PROHIBITIONS

All 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:

a. Unlawful activity.
b. Commercial or for-profit purposes
c. Non-work or non-school related work.
d. Products advertisement or political lobbying.
e. Hate mail, discriminatory remarks and offensive or inflammatory communication.
f. Unauthorized or illegal installation, distribution, reproduction or use of copyrighted materials.
g. Access to obscene or pornographic material or child pornography.
h. Inappropriate language or profanity.
i. Transmission of material likely to be offensive or

objectionable to recipients.

j. Intentional obtaining or modifying of files, passwords and data belonging to other users.
k. Impersonation of another user, anonymity and pseudonyms.
l. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
m. Loading or using unauthorized games, programs, files or other electronic media.
n. Disruption of the work of others.
o. Destruction, modification, abuse or unauthorized access to network hardware, software and files (i.e. backup).
p. Quoting of personal communications in a public forum without the original author's prior consent.
q. Unauthorized disclosure, use and dissemination of personal information regarding minors.
r. Unsupervised Chat rooms.

Student users shall not use electronic mail (e-mail) without receiving specific authorization from a teacher or Administrator.

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

6270.6. SECURITY

System security may be 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:

a. Users shall not reveal their passwords to another individual
b. Users are not to use a computer that has been logged in under another student or employee's name.
c. 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.

6270.7 COPYRIGHT/SOFTWARE

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.

6270.8 CONSEQUENCES FOR INAPPROPRIATE USE

The network user 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 of date belonging to others; copyright violations; and theft of services may be reported to the appropriate legal authorities for possible prosecution.

Loss of access and other disciplinary actions up to and including suspension or expulsion from school shall be consequences for inappropriate use.

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.

Violation of this Policy may result in disciplinary action pursuant to due process procedures established by Board Policy, state and federal law, and/or collective bargaining agreements.

6270.9 SAFETY

To the greatest extent possible, users of the network will be protected from harassment and unwanted or unsolicited communication. Any network user who received 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.

Any District computer/server utilized by students and staff shall be equipped with a technology protection measure that blocks or filters Internet access to materials that are obscene, child pornographic or harmful to minors (as those terms are defined by CIPA).

Internet safety measures shall effectively address the following:

a. Control of access by minors to inappropriate matter on the Internet and World Wide Web.
b. Safety and security of minors when using electronic mail, and other forms of direct electronic communications.
c. Prevention of unauthorized online access by minors, including “Hacking” and other unlawful activities.
d. Unauthorized disclosure, use and dissemination of personal information regarding minors.
e. Restriction of minor’s access to materials harmful to them.

The technology protection measure may be disabled by a West Allegheny School District staff member for “bon a fide” research purposes to be undertaken by an adult, provided the adult is not a secondary student.

A West Allegheny School District staff member may override the technology protection measure for a student to access a site with legitimate educational value that is wrongly blocked by the technology protection measure, provided access is not given to any obscene, child pornographic or other material harmful to minors.

6270.10 USER AGREEMENTS

The Superintendent shall develop user agreements to be executed by students, parents and staff pursuant to this Policy.

6270.11 ADDITIONAL PROVISIONS

Employees and students have “no expectation of privacy: with regard to e-mail.
Only authorized district personnel may make additions/modifications of district website files.
Administrators may develop additional guidelines to ensure efficient and proper use of the computer system and Internet.
The District reserves the right to conduct random checks to ensure compliance with this policy

6270.12 YOUR RIGHTS

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

a. You should expect only limited privacy in the contents of your personal files on the District system. The situation is similar to the rights you have in the privacy of your locker.
b. Routine maintenance and monitoring of the West Allegheny School District Internet system may lead to discovery that you have violated this policy, The SRRP, the School Code of conduct and/or the law.
c. 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.
d. Your parents have the right at any time to request to see the contents of your e-mail file.

Due Process

a. 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 Internet system.
b. 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.
c. 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.

Legal reference: Child Internet Protections Act, Federal Communications Commission regulations
Approved By Board August 21, 2002