Parkway West Career and Technology Center
7101 Steubenville Pike Oakdale, PA 15071 412-923-1772 Fax: 412-787-7257 www.parkwaywest.org

Computer, Internet, and Local Area Network Use Policy

Students are expected to act in a responsible, ethical, and legal manner in accordance with district policy, accepted rules of network conduct, and Federal and State Law when using the school's computers, networks, and/or the Internet. Prior to being offered access to Parkway's computers, networks, or the Internet, all students and their parent(s) or guardian(s) must sign a Network/Internet Usage Agreement indicating their acceptance of Parkway's policies regarding such use.

Upon satisfactory completion of the application process and completion of the Network/Internet Usage Agreement students will be issued a computer network/internet access account granting them permission to use the school's computers and networks. Any violation of school policies regarding the use of computers, networks, or the Internet may result in revocation of the computer network/Internet account and/or other disciplinary actions specified in this Handbook. In addition, any computer or network-related communications that have the potential to create a material and substantial disruption of the school's programs, whether initiated at the school, on a student's home computer, or on any other computer not on school premises, may result in disciplinary or legal action against the student.

Specifically, the following uses and attempted uses are prohibited:

1. Use of the network to facilitate illegal activity.
2. Use of the network for commercial or for-profit purpose.
3. Use of the network for non-school related work.
4. Use of the network for product advertisement or political lobbying.
5. Use of the network for hate mail, discriminatory remarks, offensive, defamatory, or inflammatory communication.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Use of the network to access obscene or pornographic material, or other material considered harmful to minors as that term is defined by law.
8. Use of text, audio and/or video web content, email, messaging, blogs, and/or discussion or social groups unrelated to class work.
9. Use of inappropriate language or profanity on the network.
10. Use of the network and/or technological means to intentionally obtain or modify files, passwords, and data belonging to other users.
11. Impersonation of another user, anonymity, and/or pseudonyms.
12. Use of the network facilities for fraudulent copying, communications, or modification of materials in violation of copyright laws.
13. Loading or using unauthorized games, programs, music, video, files, or other electronic media not specifically installed by Parkway.
14. Use of the network to disrupt the work of other users.
15. Destruction, modification, disconnection, theft, or abuse of computer and network hardware or software.
16. Accessing or attempting to access unauthorized resources.
17. Use of "tunneling", "proxy" and/or other methods to bypass the school's content filtering and network security systems.
18. Disrupting or excessively annoying other computer systems by denial of services, "phishing", "spamming", "spoofing", excessive "pinging", or other techniques.
19. Connection of any unauthorized device or equipment to any computer, printer, plotter, projector, camera or scanner, to the network.
20. Bypassing the Internet blocking filters or software (Proxies).
21. Bypassing or disabling antivirus, antispam, antimalware software.

Internet and Local Area Network Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal files. To protect the integrity of the system, the following guidelines shall apply:

1. Students shall not reveal their passwords to another individual.
2. Students are not to use a computer logged onto the network by another user. Students may be assigned to use only a particular computer, in which case they should only use that computer unless otherwise authorized.
3. Use of any other student or a teacher's login is prohibited.
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. Student network accounts and computer storage media, whether connected to or not connected to the network, are considered to be public information. Student network accounts and storage media are subject to inspection by teachers, network administrators, and school administrators at any time, for any reason, and without prior notice.
6. Information entered, copied, uploaded or downloaded to the network or computer storage media by students is not private. Logs and journals of all computer activity, network and disk access may be kept and reviewed by the school. Students who are found to have obtained, placed, or sent inappropriate, vulgar, offensive, or obscene messages, images, sounds, or any other form of information on the network, or on any computer media connected to or not connected to the network, are subject to disciplinary actions,

Internet and Local Area Network Safety

To the extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication. Parkway's Internet access is actively filtered to block content that is inappropriate or offensive. However, no guarantee can be made that a filtering system will screen all inappropriate content. Students will be held responsible for any access or attempt to access inappropriate material. Any network user who receives offensive, threatening or unwelcome communications shall immediately bring them to the attention of a teacher or an administrator.

Network users should not reveal personally identifiable information including addresses and/or telephone numbers to other users on the network. At no time will any student be permitted to divulge personal information about themselves or any other student via Internet web pages, email, blogs, social networking or any other technology while using Parkway's computers on network.

Consequences for Inappropriate or Unauthorized Use

Generally accepted rules regarding behavior and communications apply when any individual accesses the network, in addition to the provisions of this policy.

Inappropriate use of such computers or the network may result in the immediate termination of computer and network privileges and/or other disciplinary actions.

Any network user shall be responsible for damage to equipment, systems, and/or software resulting from their deliberate or willful acts.

Illegal use of the network, intentional deletion or damage to files or data belonging to others, copyright violations, and/or theft of services may be reported to law enforcement agencies for possible investigation and prosecution to the fullest extent of the law.

Vandalism of Parkway computers or equipment may also result in the immediate termination of computer and network privileges. Vandalism is defined as any malicious attempt to harm or destroy Parkway's computers, data, applications and/or network functionality or the data and/or functionality of another user's computer. This includes, but is not limited to: the uploading, downloading, or creation of any computer viruses; denial of service attacks; defacing, destroying, sabotaging, deleting, or otherwise modifying online content created by others; or bypassing and/or exploitation of computer and network security systems.