



and staff members who use the network. In general these require efficient, ethical, and legal utilization of the network resources. The use of network resources, including the Internet, is a privilege, not a right, and inappropriate use shall result in a cancellation of those privileges.

Acceptable Use

The use of the computer network must be in support of education and research and consistent with the educational objectives of the Butler Area School District. Use of network and computer resources must comply with rules appropriate for that network. Network accounts are to be used only by the authorized owner of the account for authorized purposes.

The determination as to whether a use is appropriate lies solely within the discretion of the School District.

The use of the computer network for illegal, inappropriate, or unethical purposes by students or employees is prohibited. More specifically, the following uses are prohibited:

1. Use of the network to facilitate illegal activity.
2. Use of the network for commercial or for-profit purposes.
3. Use of the network for non-work or 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, and offensive or inflammatory communication.
6. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
7. Use of the network to access obscene, sexually explicit or pornographic material.
8. Use of inappropriate language or profanity on the network.
9. Use of the network to transmit material likely to be offensive or objectionable to recipients.
10. Use of the network to intentionally obtain or modify files, passwords, and data belonging to other users.

11. Impersonation of another user, anonymity, and pseudonyms.
12. Use of network facilities for fraudulent copying, communications, or modification of materials in violation of copyright laws.
13. Loading or use of unauthorized games, screensavers, programs, files, or other electronic media.
14. Use of the network to disrupt the work of other users.
15. Destruction, modification, or abuse of network hardware and software.
16. Quoting personal communications in a public forum without the original author's prior consent.

#### 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, the following 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 teacher'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.

#### Safety and Protection of Personal Information

When sending electronic messages, students and staff shall not include personal information, such as addresses and phone numbers, that could identify themselves or other students and staff. Internet ID and passwords are provided only for personal use. Students and staff shall not share their password with anyone and shall not use anyone else's password, regardless of how the password was obtained. Those who suspect that someone has discovered their password shall change it immediately. Students and staff shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.

To the greatest extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication.



P.L. 94-553  
Sec. 107  
P.L. 106-554  
Sec. 1711, 1721,  
1732

20 U.S.C.  
Sec. 6777

PA Code  
Title 22  
Sec. 403.1

Board Policy  
814