| | |
|---|---|
| Book | Policy Manual |
| Section | 800 Operations |
| Title | Acceptable Use of Network and Internet |
| Number | 815 |
| Status | Active |
| Legal | 1. 20 U.S.C. 6777<br>2. 47 U.S.C. 254<br>3. 47 CFR 54.520<br>4. 17 U.S.C. 101 et seq<br>5. Pol. 814<br>6. 24 P.S. 4604<br>18 Pa. C.S.A. 5903<br>18 Pa. C.S.A. 6312<br>24 P.S. 1303.1-A<br>24 P.S. 4601 et seq<br>Pol. 103<br>Pol. 104<br>Pol. 218<br>Pol. 218.3<br>Pol. 220<br>Pol. 233<br>Pol. 248<br>Pol. 249<br>Pol. 348 |
| Adopted | July 9, 1997 |
| Last Revised | June 13, 2012 |

## Purpose

The Woodland Hills School District Board supports the use of the Internet and other internal or external computer networks in the district's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research and collaboration.

The use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students. The district shall make every effort to ensure that these educational resources are used responsibly by students and staff.

To meet the requirements of the Children's Internet Protection Act (CIPA), a commercially available filtering program will be applied across the district network. The district has taken available precautions to protect against access to visual depictions that are obscene, child pornographic or harmful to minors.

## Authority

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

Disclaimer

Information electronically available to students and staff does not carry endorsement of content by the school district, nor does the district guarantee the accuracy of information received on the Internet. 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 will not be responsible for any damage users may suffer due to interruptions in network service.

**Network Guests** is defined as any individual who utilizes the district's Information Technology Resources via guest network access or the guest login process.

The district shall make every effort to ensure that students, staff, and Network Guests use this resource responsibly.

## Delegation of Responsibility

Administrators, teachers and staff have a professional responsibility to work together with parents/guardians to help students develop the intellectual skills necessary to distinguish among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet the educational goals. Training and professional development will occur on an as-needed basis. This training shall include educating students about appropriate online behavior, including interacting with other individuals on social networking websites or in chat rooms, as well as cyber bullying awareness and appropriate responses.

Students, staff and Network Guests have the responsibility to respect and protect the rights of other users in the district and on the Internet.

The district Technology Department Administrator is responsible for implementing technology and procedures to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to:[1][2][3]

1. Utilizing a technology protection measure that blocks or filters Internet access by students, staff, and Network Guests to certain visual depictions that are obscene, child pornography, harmful to minors with respect to use by minors, or determined inappropriate for use by students, staff, and Network Guests.

2. Maintaining and securing a usage log.

3. Monitoring online activities of students, staff, and Network Guests.

Violations identified by the filtering program are monitored electronically and are punishable according to this policy's Consequences for Inappropriate Use section.

Recognizing that the filtering program is not fool-proof, administrators, teachers and staff have a professional responsibility to report observed incidences of access to visual depictions that are obscene, child pornographic or harmful to minors to the building principal or system administrator for action according to this policy's Consequences for Inappropriate Use section.

**Guidelines**

Conditions on Use

The Board establishes that its networks and technology and users to the Internet via those district resources are privileges, not rights; inappropriate, unauthorized or illegal use of those resources will result in the cancellation of privileges and appropriate personnel or student disciplinary action.

The district reserves the right to restrict or prevent access via its networks and other technology to sources or sites deemed inappropriate, by any means including filtering software or services, the right to log network use, the right to monitor fileserver space utilization by district users, and the right to view file content. Users should have no expectation of privacy with respect to district access to or review of file content or network utilization.

Copyright

The illegal use of copyrighted software by students and staff is prohibited. Any data up-loaded to or downloaded from the network shall be subject to fair use guidelines.[4][5]

Procedures

The district will notify the parents/guardians about the district network and policies governing its use. Elementary students' parents/guardians must sign an agreement to allow their child(ren) to have network and Internet access. Parents/Guardians may request alternate activities for their child(ren) that are not permitted Internet access.

Parents/Guardians shall have the right at any time to investigate the contents of files contained in their child(ren)'s individual account(s), and parents/guardians shall have the right to request the termination of their child(ren)'s individual account(s) at any time.

Parents/Guardians are responsible for monitoring their child(ren)'s use of the Internet while they are accessing the system from home.

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

The system administrator may close an account at any time as required. School district administration, faculty and staff may request the system administrator to deny, revoke or suspend specific user accounts. The system administrator shall have the authority to determine what is inappropriate use, and his/her decision is final.

Prohibitions

Students and staff 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. 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 nonschool related work.

4. Use of the network for product advertisement or political work.

5. Use of the network for hate mail, discriminatory remarks, and offensive or inflammatory communication.

6. Use of the network to access material that advocates illegal acts, violence or discrimination unless such access is made by an adult for bona fide research or other lawful purposes.

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

8. Use of the network to access obscene or pornographic material or child pornography.

9. Use of inappropriate language or profanity on the network.

10. Use of the network to transmit material likely to be offensive or objectionable to recipients.

11. Use of the network to intentionally obtain or modify files, passwords, and data belonging to other users.

12. Impersonation of another user, anonymity, and pseudonyms.

13. Use of network facilities for fraudulent copying, communications, or modification of materials in violation of copyright laws and/or plagiarism.[5]

14. Loading or use of unauthorized games, programs, files or other electronic media.

15. Use of the network to disrupt the work of other users.

16. Destruction, modification, abuse or unauthorized access to network hardware, software and files.

17. Quoting personal communications in a public forum without the original author's prior consent.

18. Engaging in spamming; i.e., an annoying or unnecessary message to a large number of people.

19. Access by students, staff, and Network Guests to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.

20. Use of chat rooms, message boards, guest books, Internet surveys and other forms of direct electronic communications (e.g. instant message services), except for a curriculum-related purpose, where directly monitored by teachers or staff.

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. Students, staff, and Network Guests 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.

4. Users will not attempt to gain unauthorized access to the district system or to any other computer system through the district system or go beyond their authorized access.

5. Users shall immediately notify the building principal or system administrator if they have identified a possible security problem.

Safety

To the greatest extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall immediately bring them to the attention of the building principal, teacher or systems administrator.

Network users shall not reveal at any time any personal information of a student, including but not limited to, home address, electronic mail address, user account identification, home phone number, work location, or work phone number to other users on the network or Internet, including chat rooms, email, etc.

Also, such student information shall at no time appear on district Internet or Intranet published materials. At no time shall a person accessing the district Internet/Intranet server without providing a valid user account log-in password (validated access) be able to connect a student's first or last name with a student picture or have access to first and last names of a student. Student initials only may be used on district Internet published materials with non-validated access. No pictures featuring student facial close-ups or associated names may be used on district Internet published materials with non-validated access or without parental/guardian permission.

Any district computer/server utilized by students, staff, and Network Guests shall be equipped with Internet blocking/filtering software.

Internet safety measures shall effectively address the following:[2][3]

1. Control of access by minors to inappropriate matter on the Internet and World Wide Web.

2. Safety and security of minors while using electronic mail, chat rooms and other forms of direct electronic communications.

3. Prevention of unauthorized online access by minors, including "hacking" and unauthorized activities.

4. Unauthorized disclosure, use, and dissemination of personal information regarding minors.

5. Restriction of minors' access to materials harmful to them.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.[6]

Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations or theft of services will be reported to the appropriate legal authorities for possible prosecution.

The district will cooperate fully with local, state, or federal officials in any investigation related to any illegal activities conducted through the district's computer system.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions will be consequences for inappropriate use.

Vandalism will result in disciplinary sanctions. **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, the up-loading or creation of computer viruses.

If a user unintentionally violates this policy, s/he should immediately notify the building or system administrator. This will protect users against allegations that they have intentionally violated district policy.