Policy #4116.2
Revised 11/26/08
Board Approved 12/08/08

Wilson Area School District
Acceptable Use of Internet and Computer Technology

Purpose

The Board supports use of the Internet and other computer networks 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.

For instructional purposes, 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.

Authority

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 retrieved via the Internet.

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

The district reserves the right to view and monitor all applications provided through the network, including email, to log Internet use by staff, and to monitor file server space utilization by District and outside users.

The Board establishes that network use is a privilege, not a right. Inappropriate, unauthorized and illegal use will result in cancellation of those privileges and appropriate disciplinary action.

Personnel under contract with the District, such as consultants, are bound by the terms of this policy when using the Internet within the District.

The Board establishes that the following materials, in addition to those stated in law, are inappropriate for access by minors: visual, graphic text and any other form of obscene, child pornography, or other material harmful to minors; material advocating terrorism and evil, hateful, illegal, defamatory, harassing and other materials promoting or condoning extreme violence. The School District will cooperate to the extent legally required with local, state and federal officials in any investigation concerning or related to the inappropriate use of District technology.

Delegation of Responsibility

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

Administrators, teachers and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate 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.

As required by law, the District will utilize filtering software to restrict and monitor the use of the Internet, email, blogs, and chat.

Students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet. All staff and students are responsible for reading and following this policy.

As required by law, the District will educate students about appropriate online behavior, including interacting on social networking websites and chat rooms. Furthermore, cyber bullying awareness and strategies for prevention will be integrated into instruction.

The building administrator, working in conjunction with the Superintendent, shall have the authority to determine what is inappropriate use and the consequences for inappropriate use.

The Superintendent or 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 for accessing sexually explicit materials. The procedure shall include but not be limited to:

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.

Guidelines

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 to be public. Users have no privacy expectations in the contents of

their personal files or any of their use of District technology. Network users shall respect the privacy of other users on the system.

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. Specially, the following uses are prohibited:

1. Illegal activity.

2. Uploading of School District personal and private information/data, images, and copyrighted material in blog or web page without proper consent.

3. Commercial or for-profit purposes.

4. Product advertisements or political lobbying.

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

6. Cyber bullying another individual or entity.

7. Access or transmit gambling, pools for money or any other betting or games of chance.

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

9. Access to obscene or pornographic material or child pornography.

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

11. Inappropriate language or profanity.

12. Transmission of material likely to be offensive or objectionable to recipients.

13. Participate in discussion, chat rooms or groups that cover inappropriate and/or objectionable topics or materials.

14. Intentional obtaining or modifying of files, passwords, and data belonging to other users.

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

16. Fraudulent copying, communications, or modification of materials in violation of copyright laws.

17. Bypass or attempt to bypass Internet filtering software.

18. Loading or using of unauthorized games, programs, files, or other electronic media.

19. Disruption of the work of other users.

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

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

22. Intentionally disrupting the network, network accounts, service or equipment of others.

23. Altering or attempting to alter files, systems security or software.

24. Student pictures and information in the press or electronic media, if the parent or guardian signed a release form withholding permission to publicize their son/daughter's picture.

Incidental personal use is permitted for employees as long as such use does not interfere with the employee's job duties and performance, with systems operations, or with other system users. Personal use must comply with this policy and all other applicable School District policies, procedures and rules.

Students may only use the District's network for educational purposes. The District reserves the right to revoke the privilege of remaining in or enrolling in courses that require access to technology when a student violates this policy.

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 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 are required to log off of the network when finished.

Consequences For Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts. Any and all cost incurred by the District for repairs and/or replacement of software, hardware and data files will be the responsibility of the user who has created the problem.

Illegal use of the network: intentional deletion or damage to files of data belonging to others: copyright violations; and theft of services will 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. Loss of access and other disciplinary actions 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.

Copyright

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.

Safety

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

The School District reserves the right to legally access users personal technology devices brought on to school property, or to School District events, or connected to the School District network, when the School District reasonably believes they contain information that violates a School District policy, or contain information/data that is involved in a criminal activity.

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

Internet safety measures shall effectively address the following:

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 minor's access to materials harmful to them.