Wyomissing Area School District

Book	Policy Manual
Section	800 Operations
Title	Acceptable Use of Technology Resources/Facilities and Internet by Staff, Students, and Community Members
Code	815
Status	Active
Adopted	January 27, 1997
Last Revised	November 21, 2016

Authority

The Board supports the use of the Wyomissing Area School District (WASD) network, e-mail, Internet service and other technology systems in the District's instructional and business operations to facilitate learning, teaching and daily school business through interpersonal communication, access to information, research and collaboration.[1]

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. For operational purposes, network facilities shall be used to increase productivity, enhance communication, and provide access to information for research and collaboration on District initiatives.

The use of the WASD network and technology resources is solely for the purpose of facilitating the exchange of information to further education and conduct daily business operations consistent with the mission of the School District. All District technology and content created on it are property of the District. The District has the right to supervise the use of District technology, including but not limited to, laptops, peripherals, projectors, interactive whiteboards, telephones, mobile devices and any other technological device. Any use without authorization is prohibited. Violation of any conditions of use described below will result in disciplinary action by the District. Users are responsible to indemnify the District for any and all costs associated with a violation of the Acceptable Use Policy. All users of District equipment are bound by this policy.

Access to electronic information through District resources does not imply endorsement of the content by the District; nor does the District guarantee the accuracy of information 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.

WASD reserves the right to log and monitor all District technology. This includes, but is not limited to, Internet use, computer access, network activity, e-mail and instant messaging. Any member of the Information Technology staff may review student, faculty and staff files and communication to maintain system integrity when suspicious behavior is suspected or when requested by the Superintendent. While files stored on District servers and computers are available only to the author, users should expect that these files can be viewed and monitored by IT staff when necessary.

Medical, student and personnel records are considered private and confidential. WASD reserves the right to deny access to prevent unauthorized or illegal activity at any time.

A network end-user will only use his or her own account to access District technology and resources. Network end-users shall respect the privacy of other users on the system. Use of the Internet is a privilege, not a right; inappropriate, unauthorized and illegal use will result in the loss of those privileges. Appropriate disciplinary action will also be taken.

In order for faculty, staff, School Board members and guests to use District technology, the Acceptable Use Policy must be signed. For student access, both the student and guardian must sign the policy.

Delegation of Responsibility

The District shall implement written procedures for the responsible use of this educational resource by School Board members, administration, faculty, staff, students and community members.

School Board members, administrators, faculty 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 ages and developmental levels and to evaluate and use the information relevant to the educational goals of the students.

Students and staff have the responsibility to respect and protect the rights of every other user in the District.

The Director of Information Technology in conjunction with other administrators, shall have the final authority to determine what is or is not acceptable use for School Board members, faculty, staff and students.

The Superintendent or designee shall be responsible for implementing technology and procedures to ensure that the District's computers and network are not being used for purposes prohibited by law or for accessing sexually explicit materials. The procedure shall include but not be limited to:[2][1][3]

1. Utilizing a content filter that prohibits Internet access to visual depictions that are obscene, pornographic, harmful to minors with respect to use by minors, or determined inappropriate for use by minors by the Superintendent.

2. Maintaining and securing a usage log.

3. Monitoring online activities.

Guidelines

District network accounts will be used only by the authorized owner of the account for its authorized purpose. Network users shall respect the privacy of other users on the network. Network users must agree to the District guidelines for Internet use and follow all portions of this policy.

Prohibitions

The following uses of the WASD network 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-District related work.

4. Use of the network for product advertisement, union solicitations and recruitment or political lobbying.

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

6. Unauthorized or illegal installation, distribution, reproduction or use of copyrighted materials. [7]

7. Use of the network to access obscene, pornographic, lewd or otherwise illegal material, images or photographs.[Pol]

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.

12. Installation or use of unauthorized games, programs, files or other electronic media.

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

14. Destruction, modification or abuse of network hardware and software.

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

16. Use of any data mining, bots, or similar data gathering and extraction methods in violation of any person's or entity's rights.

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. All users must respect the rights and property of others and not improperly access, misappropriate or misuse the files, data or information of others.

2. End-users are not permitted to use a computer logged in under another account. End-users may not share their individual account information with anyone.

3. Any end-user identified as a security risk may be denied access to the network.

4. All users will keep their accounts and passwords confidential. Any breach of security or violation that is tied to an end-user's account will be treated as the responsiblity of that end-user.

5. All faculty, staff and students will be required to change their passwords on a schedule defined by the IT department.

Safety (Network)

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 a teacher, staff member, administrator or appropriate school personnel.

Safety (Internet)

The District, in compliance with the federal Children's Internet Protection Act (CIPA) related to Internet filtering, adheres to the following safety measures:[1][3]

1. The District utilizes a content filter to filter Internet access and to protect against access to visual depictions by adults and minors that are obscene, child pornography or – with respect to computers with Internet access by minors – harmful to minors. Faculty and staff members may submit websites that are blocked by the Internet filter for the IT department's review. The IT staff will review the site and grant access to the site if it is appropriate.

2. Student use of the Internet in the schools will be monitored by a responsible adult such as the teacher, librarian or a classroom/library aide. Student activity will also be logged by the IT staff and history will be available upon request by an administrator.

3. Software and hardware protections will be instituted in order to prevent unauthorized access, including hacking and other unlawful activities, by minors or by adults online.

4. The use of personally identifiable information related to minors will not be allowed for display on publicly available District resources without consent. This information includes, but is not limited to, full names, addresses, telephone numbers, photos, etc.

5. As pursuant to the Protecting Children in the 21st Century Act, WASD is committed to educating students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response. The School District will educate all students about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms and cyberbullying awareness and response.[4]

6. Students shall not reveal their personal full names, addresses or telephone numbers to other users on the Internet.

Software & Hardware

1. All users are responsible for taking precautions to prevent the introduction of viruses to the WASD network. Attempts to degrade or disrupt any District computer or network system performance by spreading computer viruses is considered criminal activity under state, federal, and local law.

2. The unauthorized purchase, download or installation of software or files for use on District computers is prohibited. Software may not be installed by anyone other than a member of the IT Department.

3. Users of District software shall abide by the software licensing agreement provided by the software publisher. Software piracy, the illegal use or possession of copyrighted software, is strictly prohibited.

4. Connecting a non-District owned device to a District computer or the District network is prohibited unless authorized in writing by the Director of Information Technology.

5. Defacing District technology is prohibited. This includes, but is not limited to, marking equipment with pens, pencils, whiteout, and stickers, as well as the removal of District or equipment manufacturer labels, logos, and asset tags.

6. District owned devices will be operated within the specifications provided by the respective manufacturer; and

7. File storage on the network or district-provided internet resource is limited to schoolwork only unless authorized in writing by the Director of Information Technology.

Confidentiality

No confidentiality or privacy is represented or guaranteed by the School District for employee or student use of the District's technology systems. Consequently, messages transmitted or otherwise conveyed by these systems are not and should not be considered private. Any party who uses Wyomissing Area School District's technology systems to transmit or receive communications shall be deemed to have consented to having the content of any such communications reviewed by the Wyomissing Area School District. The School District reserves the right to monitor network use at any time, without notice.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems and software resulting from deliberate or willful acts.[5]

The network user shall be responsible for computing devices that travel between buildings and between buildings and the user's home. If a theft occurs, proper filing with police and insurance agencies should be coordinated with the Director of Information Technology.

Illegal use of the network, intentional deletion or damage to files of data belonging to the School District or others; copyright violations or theft of services will be reported to the appropriate authorities.

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 can be consequences for inappropriate use.

Vandalism can result in cancellation of access privileges and other disciplinary actions. **Vandalism** is defined as any attempt to harm or destroy data of the School District or another user, Internet or other networks. This includes but is not limited to the uploading or creation of computer viruses.

A discipline policy is established at each building that addresses violations of this policy. Each violation will be handled on a case-by-case basis. Building administrators and his/her designee will confer with the Director of Technology Services in terms of access and privileges to District computers systems and network and will report all infractions to the Superintendent.

Copyright

The illegal use of copyrighted software by students, faculty, administrators, staff, and School Board members is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines.[8][7]

All users must respect copyright and fair use guidelines when using the WASD network. This includes, but is not limited to:

1. Copyright material must be used in accordance with the Fair Use Doctrine, the TEACH Act and pertinent District policy and regulations.

2. Teachers posting materials to teacher web sites, blogs, wikis, social networking systems and other online resources must conform to the same Fair Use Doctrine, TEACH Act and pertinent District policies and procedures.

The administration and IT department have the right to monitor these services for copyright violations and take appropriate action against violators.

Establishment of Web Sites

1. The District may establish a web site and develop web pages that present information about the District. The Director of Information Technology, or his/her designee, will be responsible for maintaining the District Web site.

2. Schools or classes may establish Web pages that present information about the school or class activities. The IT Department has the right to monitor and or remove content that is not appropriate. In addition, web pages shall be created within the guidelines set forth in other provisions of this policy and within the style/administrative guidelines developed by the Director of Information Technology. Teachers will be responsible for maintaining such web pages utilizing procedures developed by the Director of Technology Services.

3. With the approval of the Director of Information Technology, co-curricular clubs or teams may establish web pages. The building principal may request to approve the content of the web page before it is published. In addition, web pages shall be created within the guidelines set forth in other provisions of this policy and within the style/administrative guidelines developed by the Director of Information Technology. Teachers or other staff members serving as activity sponsors or coaches will be responsible for maintaining such web pages utilizing procedures developed by the Director of Information Technology.

Social Networking and Social Media

1. Communication between District employees and current WASD students through social networking sites/services not hosted or sponsored by the District is prohibited without administrative approval by the Superintendent or designee.

2. Use of the District’s logo or seal on social networking sites is prohibited unless permission is granted in writing by the Director of Information Technology.

3. Defaming or otherwise discrediting the District is prohibited.

4. Mentioning the names of students is prohibited.

The Wyomissing Area School District will rigorously uphold laws pertaining to the use of technological equipment and the information contained in them or generated by its use. Anyone found to be violating such laws will be subject to further disciplinary action and may be reported to appropriate authorities. Damage to equipment may result in reimbursement to the District for loss and/or repair at the discretion of the Director of Information Technology.

Legal

1. 47 U.S.C. 254
2. 20 U.S.C. 6777
3. 47 CFR 54.520
4. Pol. 249
5. 24 P.S. 4604
7. Pol. 814
8. 17 U.S.C. 101 et seq

24 P.S. 1303.1-A

18 Pa. C.S.A. 5903

18 Pa. C.S.A. 6312

24 P.S. 4601 et seq

18 U.S.C. 2256

Pol. 103

Pol. 103.1

Pol. 104

Pol. 218

Pol. 218.2

Pol. 220

Pol. 233

Pol. 237

Pol. 317

Pol. 417

Pol. 517