Waynesboro Area School District

Your Child's Online Footprint

The Waynesboro Area School District is proud of the programs that are provided to students, families and the community. The District is pleased to share these learning experiences and activities provided in the district with the world at large through the use of our district website and social media. Each person builds their digital footprint when pictures, images and text are posted about them. The Waynesboro Area School District would like to help your child build his or her digital footprint in a positive way.

Dear Parent(s)/Guardian(s)/Students,

Waynesboro Area School District maintains a website and social media presence that allows the district to communicate with the community and the world. Student work and student images may be published on the website and social media only as they relate to a class project, course or other school related activity. Only the first name, or first name and last initial, of students may be used on the website. Documents may not include a student's phone number, address, names of other family members or names of friends. Web page and social media documents may not include any information that indicates the physical location of a student at a given time, other than attendance at a particular school or activity. Web pages may not contain any individual student e-mail address links or any other type of direct response links.

When a student and parent/guardian sign this policy, it remains in effect until he/she graduates from the District. You can change your consent level at any time by contacting a building secretary. This form is available on the District's web page at www.wasd.k12.pa.us.

Sincerely,

Dr. Tod F. Kline

Superintendent
Waynesboro Area School District

_____ I do consent to my child's name, likeness, image or work being published
_____ I do not consent to my child's name, likeness, image or work being published

Student Name: _____ Grade /Teacher. _____ _____ School _____

Parent/Guardian Name: _____ Date: _____

Parent/Guardian Signature: _____

Date: _____

For Office Use Only
Date entered into Sapphire: _____

WAYNESBORO AREA SCHOOL DISTRICT
ACCEPTABLE USE POLICY (AUP)

Student User Agreement

Dear Parent(s)/Guardian(s)/Students,

The Waynesboro Area School District is committed to the appropriate and engaging use of technology to enhance learning and to foster creativity. Through the Acceptable Use Policy (AUP), students are encouraged to be both responsible producers and consumers of information when using any devices (personal or school-owned) while on school property.

In the Waynesboro Area School District, all students are required to sign the AUP Policy when they enroll in school. **When a student and parent/guardian sign this policy, it remains in effect until he/she graduates from the District.** Please review the attached Board Policy 815 with your child(ren) and discuss its importance. By following the rules set forth in the policy your child(ren) will help ensure his/her safety while using the Internet.

Sincerely,

Dr. Tod F. Kline, Superintendent

I acknowledge that I have received and read the Waynesboro Area School District's Acceptable Use of Technology Policy for Students, recognize its importance and understand this policy governs my use of the district networks and Internet. I have been instructed to read and adhere to the provisions of this policy. Additionally, I understand that if I violate the policy, I am subject to district discipline and could be subject to Internet Service Provider (ISP), as well as local, state and federal legal recourse. I agree to comply with the Waynesboro Area School District's Acceptable Use of Technology Policy for Students.

Student's Signature:_____ Date: _____

School:_____ Grade:_____

Student's Name Printed: _____

I acknowledge that I have received and reviewed the Waynesboro Area School District's Acceptable Use of Technology Policy for Students, recognize its importance and understand this policy governs my child's use of the district network and Internet.

Parent(s)/Guardian(s) Signature: _____

Date: _____

Return this sheet to your child's homeroom teacher.

For Office Use Only
Date entered into SIS:
-

Book
Policy Manual

Section
800 Operations

Title
Acceptable Use of Technology Resources

Number
815

Status
Active

Legal
1. 20 U.S.C. 6777
2. 47 U.S.C. 254
3. Pol. 218
4. Pol. 233
5. Pol. 317
6. Pol. 248
7. Pol. 348
8. Pol. 103
9. Pol. 103.1
10. Pol. 104
11. Pol. 249
12. Pol. 218.2
13. 24 P.S. 4604
14. 24 P.S. 4610
15. Pol. 237
16. 47 CFR 54.520
17. 24 P.S. 1303.1-A
18. Pol. 814
19. Pol. 800
20. Pol. 216
21. 18 U.S.C. 2256
22. 18 Pa. C.S.A. 6312
23. 18 Pa. C.S.A. 5903
24. 17 U.S.C. 101 et seq
24 P.S. 4601 et seq
Pol. 220

Adopted
July 25, 2017

Purpose

The Waynesboro Area School District provides its employees, students and guests ("Users") access to technology resources including, but not limited to, electronic communications systems, computers, computer networks, networked devices, hardware, software, Internet access, mobile devices, peripherals, copiers, and cameras.

The Board supports the use of the district's technology resources to facilitate teaching and learning, to provide access to information, to aide in research and collaboration, to foster that educational mission or the district, and to carry out legitimate business and operation of the district, and to carry out the legitimate business and operation of the district.

The use of the district's technology resources is for appropriate school-related educational and operational purposes and for the performance of job duties consistent with the educational mission of the district. **Use of educational purposes** is defined as use that is consistent with the curriculum adopted by the district, as well as the varied instructional needs, learning styles, abilities and developmental levels of students. All use for any purpose must comply with this policy and all other applicable codes of conduct, policies, procedures, and rules and must not cause damage to the district's technology resources.

All employees and students are responsible for the appropriate and lawful use of the district's technology resources. This policy is intended to ensure that all Users continue to enjoy access to the district's technology resources and that such resources are utilized in an appropriate manner and for legitimate purposes.

Definitions

District Technology Resources - district technology resources means all technology owned and/or operated by the district, including computers, projectors, televisions, video and sound systems, mobile devices, calculators, scanners, printers, cameras, portable hard drives, hardware, software, routers, and networks, including the Internet.

User - User means anyone who utilizes or attempts to utilize district technology resources while on or off district property. The term includes, but is not limited to, students, staff, parents/guardians, and any visitors to the district that may use district technology.

Access to the Internet - a device shall be considered to have access to the Internet if the device is connected to a network that has access to the Internet, whether by wire, wireless, cable or any other means.

Child pornography - under federal law, any visual depiction, including any photograph, film, video, picture, or computer or computer-generated image or picture, whether made or produced by electronic, mechanical, or other means, of sexually explicit conduct, where:[21]

1. The production of such visual depiction involves the use of a minor engaging in sexually explicit conduct;

2. Such visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaging in sexually explicit conduct; or

3. Such visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaging in sexually explicit conduct.

Under Pennsylvania law, any book, magazine, pamphlet, slide, photograph, film, videotape, computer depiction or other material depicting a child under the age of eighteen (18) years engaging in a prohibited sexual act or in the simulation of such act is considered child pornography.[22]

Electronic devices - any school district-owned, leased or licensed or User owned: personal hardware, software, or other technology used on school district premises or at school district events, connected to the school district Technology Systems, and/or containing school district programs or data. Electronic devices include, but are not limited to, laptops, desktops, cell phones, external media, wireless devices and similar technologies.

Electronic communications systems - any messaging, collaboration, publishing, broadcast, or distribution system that depends on electronic communications resources to create, send, forward, reply to, transmit, store, hold, copy, download, display, view, read, or print electronic records for purposes of communication across electronic communications network systems between or among individuals or groups, that is either explicitly denoted as a system for electronic communications or is implicitly used for such purposes.

Educational purpose - includes use of the Technology Systems for classroom activities, professional or career development, and to support the school district's curriculum, policy and mission statement.

Guest - shall mean, but may not be limited to, visitors, guests, adult education attendees, workshop attendees, contractors and other individuals authorized to use the district's technology resources.

Harmful to minors - under federal law, any picture, image, graphic image file or other visual depictions that:[1][2]

1. Taken as a whole, with respect to minors, appeals to the prurient interest in nudity, sex, or excretion;

2. Depicts describes, or represents in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual content, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals, and

3. Taken as a whole lacks serious literary, artistic, political, or scientific value as to minors.

Under Pennsylvania law, any depiction or representation in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:[23]

1. Predominantly appeals to the prurient, shameful, or morbid interest of minors;

2. Is patently offensive to prevailing standards in the adult community as a whole with respect to what is suitable material for minors; and

3. Taken as a whole, lacks serious literary artistic, political, educational or scientific value for minors.

For purposes of this policy, any text or audio depictions of such matters shall be included in this definition.

Inappropriate matter - inappropriate matter includes, but is not limited to, visual, graphic, text and other form of obscene, sexually explicit, child pornographic, or other material that is harmful to minors, hateful, illegal, defamatory, lewd, vulgar, profane, rude, inflammatory, threatening, harassing, discriminatory (as it pertains to race, color, religion, national origin, gender, material status, age, sexual orientation, political beliefs, receipt of financial aid, or disability), violent, bullying, terroristic, and/or advocates the destruction of property.

Incidental personal use - use of school district Technology Systems by an individual User for occasional personal communications.

Minor - for purposes of compliance with the Children's Internet Protection Act ("CIPA"), an individual who has not yet attained the age of seventeen (17). For other purposes, minor shall mean any person under the age of eighteen (18).

Network - a system that links two (2) or more electronic devices, including all components necessary to effect the operation.

Obscene - under federal and Pennsylvania law, any material if:[23]

1. The average person, applying contemporary community standards, would find that the material, taken as a whole, appeals to the prurient interest;

2. The subject matter depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and

3. The subject matter, taken as a whole, lacks serious artistic, political educational or scientific value.

School district premises - school district premises shall include all buildings, facilities, parking areas and other grounds, owned or leased by the school district and/or otherwise under the

control of the school district, as well as all school buses, school vehicles and other conveyances used to transport school district students.

Sexual act and sexual contact - as defined at 18 U.S.C. § 2246(2), 18 U.S.C. § 2246(3), and 18 Pa. C.S.A. § 5903.

Un-authorized Use Prohibited - Only Users who have agreed to abide by the terms of this policy may utilize the district's technology resources. Unauthorized use, utilizing another district account, or exceeding one's authorization to use district technology resources is prohibited.

Use of Personal Electronic Devices - The use of personal electronic devices on the district network is permitted only on designated networks. When a User connects a personal electronic device to a district network or district technology resources, this policy and its guidelines apply. Users are subject to the same levels of monitoring and access as if a district-owned device were being utilized. Users who connect a personal electronic device to a district network explicitly waive any expectation of privacy in the content exchanged over the district technology resources.

Privacy - The district reserves the right to monitor any User's utilization of district technology resources. Users have no expectation of privacy while using district technology resources whether on or off district property. The district may monitor, inspect, copy, and review and and all usage of district technology resources including information transmitted and received via the Internet to ensure compliance with this and other district policies, and state and federal law. All emails and message, as well as any files stored on district technology resources may be inspected at any time for any reason.

Internet Filtering and CIPA Compliance - The district utilizes content and message filters to prevent Users from accessing material through district technology resources that has been determined to be obscene, offense, pornographic, harmful to minors, or otherwise inconsistent with the district's educational mission. The Superintendent or technology director shall establish a procedure for Users to request that a legitimate website or educational resource not be blocked by the district's filters for a bona fide educational purpose.

The Board directs that the Superintendent or the technology director ensure that students at the elementary, middle school and high levels are educated about appropriate online behavior including interacting via social networks and in chat rooms, cyberbullying, and disclosure of personal information

Monitoring - district technology resources shall be periodically monitored to ensure compliance with this and other district policies including monitoring of Users' online activities. The network administrator designated by the Superintendent shall ensure that regular monitoring is completed pursuant to this section. However, the Superintendent, or technology director, shall also implement procedures to ensure that district technology resources are not utilized to track the whereabouts or movements of individuals, and that remotely activated cameras and/or audio are not utilized except where necessary to recover lost or stolen district technology.

District Provided Resources - district technology resources may be assigned or allocated to an individual User for his/her use (e.g. individual email accounts, laptop computers, etc.) Despite being allocated to a particular User, the technology resources remain the property of the district and may be revoked, suspended, or inspected at any time to ensure compliance with this and other district policies. Users do not have an expectation of privacy in any district provided technology resource or any of its contents.

Authority

The availability of access to electronic information does not imply or express endorsement by the district of the content, nor does the district guarantee or warranty 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 makes no warranties of any kind, whether express or implied, for the service it is providing through its various technology resources. The district is not responsible for any damages, including loss of data resulting from delays, non-deliveries, missed deliveries, or services interruption.

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

The Board declares that Internet, computer, systems and network use is a privilege, not a right. The district's computer, systems and network resources are the property of the district. Users shall have no expectation of privacy in anything they create, store, send, delete, receive or display on or over the district's technology resources, including personal files or any use of the district's Internet, computers, systems or network resources. The district reserves the right to monitor, track, and log network access and use; monitor fileserver space utilization by district Users; or deny access to prevent unauthorized, inappropriate or illegal activity and may revoke access privileges and/or administer appropriate disciplinary action. The district shall cooperate to the extent legally required with the Internet Service Provider (ISP), local, state and federal officials in any investigation concerning or related to the misuse of the district's technology resources.[3][4][5]

The Board requires all Users to fully comply with this policy and to immediately report any violations or suspicious activities to the Superintendent or designee.

The Board establishes the following materials, in addition to those stated in law and defined in this policy, that are inappropriate for access by minors:[2]

1. Defamatory
2. Lewd, vulgar, or profane.
3. Explicit graphics.
4. Obscene text.
5. Sexually explicit.
6. Pornographic material that is harmful to minors.
7. Threatening.

8. Harassing.[6][7]
9. Discriminatory, in accordance with Board policy.[8][9][10]
10. Bullying.[11]
11. Terroristic.[12]

The district reserves the right to restrict access to any Internet sites or functions it deems inappropriate through established Board policy, or the use of software and/or online server blocking. Specifically, the district operates and enforces a technology protection measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The technology protection measure shall be enforced during use of computers with Internet access.[1][2][13]

The district shall not guarantee or warranty the effectiveness of the technology protection measure(s).

Upon request by students or staff, the Superintendent or designee shall expedite a review and may authorize the disabling of Internet blocking/filtering software to enable access to material that is blocked through technology protection measures but is not prohibited by this policy.[13]

Upon request by students or staff, building administrators may authorize the temporary disabling of Internet blocking/filtering software to enable access for bona fide research or for other lawful purposes.[1][14]

The district reserves the right to limit or restrict use of district low priority technology during situations in which network and computing requirements exceed available capacity, in accordance with the following usage priorities:

1. Highest – Directly supports the education of students.

2. Medium – Indirectly benefits the education of students.

3. Lowest – Reasonable and limited educational interpersonal and incidental personnel communications.

4. Forbidden – Activities in violation of policy.

Delegation of Responsibility

The district shall make every effort to ensure that technology resources shall be used responsibly by students and staff.

Students may not utilize district technology without the approval and supervision of designated staff.

The district shall inform staff, students, parents/guardians and other Users about this policy through employee and student handbooks, posting on the district website, and by other

appropriate methods. A copy of this policy shall be provided to parents/guardians, upon written request.[13]

Users of district networks or district-owned equipment shall, prior to being given access or being issued equipment, sign User agreements acknowledging awareness of the provisions of this policy, and awareness that the district uses monitoring systems to monitor and detect inappropriate use and tracking systems to track and recover lost or stolen equipment.

Student User agreements shall also be signed by a parent/guardian.

The connection of personal electronic devices to the district's Internet, systems and/or network shall require the prior approval of designated building administrator(s).[15]

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

Parents/Guardians shall be responsible for educating and communicating to their child their expectations regarding use of technology.

Students, staff and other authorized Users shall be responsible for the following:

1. Respecting and protecting the rights of every other User in the district and on the Internet.

2. Proving immediate notification to the Director of Technology or designee or a building administrator regarding suspected breach of security protocols.

Building administrators shall make initial determinations of whether inappropriate use has occurred.

The Superintendent or designee shall be responsible for recommending technology and developing procedures used to determine whether the district's computers are being used for purposes prohibited by law or for accessing sexually explicit materials. The procedures shall include but not be limited to:[1][2][16]

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.

The Superintendent or designee shall develop and implement administrative regulations that ensure students are educated on network etiquette and other appropriate online behavior, including:[2]

1. Interaction with other individuals on social networking websites and in chat rooms.

2. Cyberbullying awareness and response.[11][17]

Guidelines

Network accounts shall be used only by the authorized owner of the account for its approved purpose. Network Users shall respect the privacy of other Users on the system.

The Director of Technology or designee shall be responsible for the establishment, development and/or maintenance of the following:

1. Individual and class accounts
2. Quotas for User access.
3. Retention schedules.
4. Virus protection process.

Safety

It is the district's goal to protect Users of the network from harassment and unwanted or unsolicited electronic communications. Any network User who receives threatening or unwelcome electronic communications or inadvertently visits or accesses an inappropriate site shall report such immediately to a teacher, administrator or the Director of Technology or designee. Network Users shall not reveal personal information to other Users on the network, including chat rooms, email, social networking websites, etc.

Internet safety measures shall effectively address the following:[2][16]

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 minors' access to materials harmful to them.

General Prohibitions - The following uses of district technology resources are prohibited:

1. Use of technology resources to violate the law, facilitate illegal activity, or to encourage others to do so.

2. Use of technology resources to violate any other district policy.

3. Use of technology resources to engage in any intentional act which might threaten the health, safety, or welfare of any person or persons.

4. Use of technology resources to cause, or threaten to cause harm to others or damage to their property.

5. Use of technology resources to bully, or to communicate terroristic threats, discriminatory remarks, or hate.[11][17]

6. Use of technology resources to communicate words, photos, videos, or other depictions that are obscene, indecent, vulgar, rude, profane, or that advocate illegal drug use.

7. Use of technology resources to create, access, or to distribute obscene, profane, lewd, vulgar, pornographic, harassing, or terroristic materials, firearms, or drug paraphernalia.[15]

8. Use of technology resources to attempt to interfere with or disrupt district technology systems, networks, services, or equipment including, but not limited to, the propagation of computer "viruses" and "worms," Trojan Horse and trapdoor program codes.

9. Altering or attempting to alter other Users' or system files, system security software, system or component settings, or the systems themselves, without authorization.

10. The attempted physical hard or attempted destruction of district technology resources.

11. Use of technology resources in a manner that jeopardizes the security of the district's technology resources, or in a manner that attempts to circumvent any system security measures.

12. Use of technology resources to intentionally obtain or modify files, passwords, and/or data belonging to other Users or to the district.

13. Use that conceals or attempts to conceal a User's identity, including the use of anonymizers, or impersonation of another User.

14. Unauthorized access, interference, possession, or distribution of confidential or private information.

15. Using technology resources to send any district information to another party, except in the ordinary course of business as necessary or appropriate for the advancement of the district's business or educational interests.

16. Use of technology resources to commit plagiarism.[18]

17. Installing, loading, or running software programs, applications, or utilities not explicitly authorized by district technology staff.

18. Installing unauthorized computer hardware, peripheral devices, network hardware, or system hardware onto technology resources.

19. Copying district software without express authorization from a member of the district's technology staff.

20. Use of technology resources for commercial purposes.

21. Use of technology resources for political lobbying or campaigning, not including student elections (e.g. student government, club officers, homecoming queen, etc.).

22. Use of district technology resources to tether or otherwise connect to a nondistrict-owned device to access an unfiltered and/or unmonitored Internet connection.

23. The use of proxies or other means to by pass Internet content filters and monitoring.

24. The use of technology resources to gamble.

25. Unauthorized access into a restricted system or changing settings or access rights to a restricted system or account.

26. The use of encryption software that has not been previously approved by the district.

27. Sending unsolicited mass-email messages, also known as spam.

28. Scanning the district's technology resources for security vulnerabilities.

29. Sharing one's Username or password or using someone else's Username or password.

30. Sending protected student information or district communication to an employee's or another individual's private or personal email accounts to circumvent district policies or procedures.

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, these guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.

2. Users are not to use a computer and/or account 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.

Records

The management and removal of email, files and electronic information which utilizes excess technology resource space shall be in accordance with Board policy.[19]

Copyright

The illegal use of copyrighted materials is prohibited. Any data uploaded to or downloaded from the network shall be subject to fair use guidelines and applicable laws and regulations.[18][24]

District Website

The district shall establish and maintain a website and shall develop and modify its web pages to present information about the district under the direction of the Superintendent or designee. All Users publishing content on the district website shall comply with this and other applicable district policies.

Users shall not copy or download information from the district website and disseminate such information on unauthorized web pages without authorization from the building administrator.

Student Developed Website

The district may allow students the opportunity to develop and publish content on the district's website in accordance with the following:

1. Student web pages profiling a student shall be prohibited. A web page shall not contain a student's phone number, address, email, club/team membership, opinions or other personal profile information.[20]

2. Blogs, wikis and podcasts created by students shall follow the direction provided by the teacher, be for educational purposes only and comply with Board policy.

3. All content shall be reviewed by a teacher or administrator prior to posting.

4. Blogs, wikis and other communication forums shall be supervised by a teacher or administrator.

Consequences for Inappropriate Use

Damage that is a result of negligence are not covered by the manufacturer warranty. Under these circumstances the student will be required to pay a fee to repair/replace the laptop. Repeated incidents of repair/replacement by an individual will result in disciplinary measures. Students shall report all laptop issues to a teacher or the school's Student-Run Help Desk. All technical incidents will be entered into a help ticket system and tracked.[13]

Replacement and repair fees will be charged for damage that is a result of negligence. All unpaid fees will remain on the student's record and may result in a restriction to school events and records until all fees are paid.

Incidents of theft occurring off campus must be reported to the police by the parent or student. A copy of the police report must be brought to the school and be given to school administration. Any theft occurring on school grounds must be reported to the main office.

The district will work the Waynesboro Area School District Police Officer to report all model, asset, and serial numbers of stolen or lost Chromebooks to local pawn shops and area law enforcement agencies.

Illegal use of the network; intentional deletion or damage to files or data belonging to others; copyright violations; and theft of services shall 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.

Vandalism shall result in temporary or permanent loss of access privileges, disciplinary action(s), and/or legal proceedings. **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.

Failure to comply with this policy or inappropriate use of the district’s technology resources shall result in usage restrictions, loss of access privileges, financial restitution, disciplinary action(s) and/or legal proceedings.[3][4][5]