WILMINGTON AREA SCHOOL DISTRICT

SECTION: OPERATIONS

TITLE: ACCEPTABLE USE OF TECHNOLOGY

ADOPTED: January 19, 2015

REVISED: February 13th, 2017

815. ACCEPTABLE USE OF TECHNOLOGY

1. Purpose

Wilmington Area School District (herein referred to as "the District") acknowledges the value of technology in educational environments and supports the District's use of technology in curriculum.

The Board supports the use of computers, software, internet, electronic communication, and other network resources (herein referred collectively as "Technology") and provides students, faculty, staff, and other authorized individuals (herein referred collectively as "Users") with access to the District's technology to facilitate learning, teaching, and daily operations through interpersonal communications and access to information, research, and collaboration tools.

2. Definitions

Internet Access – the ability and process of an Electronic Device to connect to the internet.

Electronic Devices - any school district owned, leased, licensed, or user owned personal electronic hardware or other technological device. Electronic devices include, but are not limited to, laptops, desktops, cell phones, external media, wireless devices and similar technologies.

18 U.S.C. Sec. 2256

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

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

18 Pa. C.S.A. Sec. 6312

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.

* The term child pornography is defined under both federal and state law.

20 U.S.C. Sec. 6777

Harmful to minors - under Federal Law, is any picture, image, graphic image file or other visual depiction that:

1. Taken as a whole, with respect to minors, appeals to a 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 contact, actual or simulated normal or perverted sexual acts, or lewd exhibition of the genitals;
3. Taken as a whole lacks serious literary, artistic, political, educational or scientific value for minors.

18 Pa. C.S.A. Sec. 5903

Harmful to minors – under Pennsylvania State Law, means any description or representation, in whatever form, of nudity, sexual conduct, sexual excitement, or sadomasochistic abuse, when it:

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

18 Pa. C.S.A. Sec. 5903

Obscene - any material or performance, if:

1. The average person applying contemporary community standards would find that the subject matter 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 depicts or describes in a patently offensive way, sexual conduct described in the law to be obscene; and

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

47 U.S.C. Sec. 254

Web Filtering or **Technology Protection Measure** - a specific technology that blocks or filters Internet Access to visual depictions that are obscene, Child Pornography, or Harmful to Minors, or threatens the security or integrity of District technology or data.

Vandalism - the intentional, reckless, malicious, and/or negligent destruction, or damage, to property.

Incidental Personal Use - use of District Technology by an individual user for occasional personal communications.

18 Pa. C.S.A. Sec. 5903

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 facilitate communication between said devices.

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 District owned/operated conveyances used to transport School District students or personnel.

18 U.S.C. Sec. 2510

Electronic Communication – including, but not limited to, the transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system. Examples: electronic mail (e-mail), Instant Message (IM), Short Message Service (SMS, aka "Text message"), Multimedia Messaging Service (MMS)

Cloud Storage – any digital medium in which electronic data is stored and/or accessed outside of the WASD owned network.

3. Usage

The District's Technology is provided primarily for education related purposes and official district operations. Incidental personal use of District Technology is permitted so long as such use does not interfere with educational practices, operations, or with other technology users. Personal use must comply with this policy and with all other applicable District policies, procedures, and rules, as well as all local, state, and federal laws. Personal use of District Technology is a privilege and may be revoked at any time should it cause damage to or impair District technology, or for any reason determined by the School District.

Authorized individuals may also be permitted to use personally owned electronic devices such as laptops, tablets, and mobile phones. These devices must be approved for use by the Superintendent, School Principal and the District's Technology Manager/Coordinator. Personal devices must comply with the same policies, procedures, and rules as devices owned by the District while on school property or connected in any way to District Technology.

4. Security

The Technology Department of the Wilmington Area School District will endeavor to protect District Technology and its users from numerous external and internal risks and vulnerabilities including, but not limited to, viruses, malware, inappropriate content, and malicious activity. The Technology Department recognizes users as important contributors in protecting District Technology and assets. Users are required to fully comply with all technology related policies to help protect against security risks and vulnerabilities. Users are also required to report any violations or suspicious activity to the Technology Department or School Principal immediately.

5. Authority

The Board declares that computer and network use is a privilege, not a right. The District's computer 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 electronic devices or network. The District reserves the right to monitor, track, and log network access and usage, monitor fileserver space utilization, 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 Internet, computers and network resources.

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. Enforcement of compliance shall be defined and detailed in Administrative Regulation #815 (Board Policy 815-AR)

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

Policy 103, 103.1, 104, 248, 348

Policy 249

Policy 218.2

1. Defamatory.
2. Lewd, vulgar, or profane.
3. Threatening.
4. Harassing or discriminatory.
5. Bullying.

6. Terroristic.

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 Web Filtering measure(s) that blocks or filters access to inappropriate matter by minors on its computers used and accessible to adults and students. The Web Filtering measure shall be enforced during use of District technology.

6. 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.

Safety

47 U.S.C Sec. 254

47 C.F.R. Sec. 54.520

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 his or her immediate supervisor or administrator. 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:

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.

Prohibitions

Users 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. Facilitating illegal activity.
2. Commercial or for-profit purposes.
3. Non-work or non-school related work not excluded in section #3
4. Product advertisement or political lobbying.
5. Bullying or Cyberbullying.

SC 1303.1-A

6. Hate mail, discriminatory remarks, and offensive or inflammatory communication.
7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
8. Accessing, sending, receiving, transferring, viewing, sharing or downloading obscene, pornographic, lewd, or otherwise illegal materials, images or photographs.
9. Access by students and minors to material that is harmful to minors or is determined inappropriate for minors in accordance with Board policy.
10. Inappropriate language or profanity.
11. Transmission of material likely to be offensive or objectionable to recipients.
12. Intentional obtaining or modifying of files, passwords, and data belonging to other users.
13. Impersonation of another user, anonymity, and pseudonyms.

Policy 814

14. Fraudulent copying, communications, or modification of materials in violation of copyright laws.
15. Loading or using of unauthorized games, programs, files, or other electronic media.
16. Disruption of the work of other users.
17. Destruction, modification, vandalism, abuse, or unauthorized access to network hardware, software and files.
18. Accessing the Internet, District computers or other network resources without authorization.
19. Disabling or bypassing the Internet blocking/filtering software without authorization.
20. Accessing, sending, receiving, transferring, viewing, sharing or downloading confidential information without authorization.
21. Quoting of personal communications in a public forum without the original author's prior consent.
22. Use of all Cloud Storage services for work or academic purposes other than the District's provided service.
23. Use of personal email for school related communication by any employee.
24. Use of District technology to send unsolicited or chain emails.

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 District technology, these guidelines shall be followed:

1. Users, not limited to: 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 unless caused by extenuating circumstances.

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 may not use any hardware, software, or any other means to bypass, thwart, or compromise District technology protection measures including, but not limited to, network firewalls, web filtering policies, anti-virus measures, camera systems, and electronic door mechanisms.
5. Employees of the District may not store electronic files or email in Cloud Services outside of the managed service provided by the WASD Technology Department when those files are related to their employment in anyway.

17 U.S.C. Sec. 101

Policy 814

Copyright

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

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 principal.

Web pages created by a teacher or student for curricular purposes shall comply with this policy

Consequences for Inappropriate Use

The user shall be responsible for damages to the equipment, systems, and software resulting from deliberate, willful, negligent, or other acts as defined as Vandalism.

24 P.S. Sec. 4604

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 authorities for disciplinary action and/or legal prosecution disciplinary action.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy.

Policy 218, 233, 317

Vandalism shall result in loss of access privileges, disciplinary action, and/or legal proceedings.

Failure to comply with this policy or inappropriate use of the Internet, District network, or devices shall result in usage restrictions, loss of access privileges, disciplinary action, and/or legal proceedings.

School District Limitation Of Liability

The School District makes no warranties of any kind, either expressed or implied, that the functions or the services provided by or through the School District's Technology Systems will be error- free or without defect. The School District does not guarantee the effectiveness of Internet filtering. The electronic information available to users does not imply endorsement of the content by the School District, nor is the School District responsible for the accuracy or quality of the information obtained through or stored on the Technology Systems. The School District shall not be responsible for any damage users may suffer, including but not limited to, information or equipment that may be lost, damaged, delayed, misdelivered, or unavailable when using electronic devices. The School District shall not be responsible for material that is retrieved through the Internet, or the consequences that may result from them. The School District shall not be responsible for any unauthorized financial obligations, charges or fees resulting from or through access to the School District's Technology Systems. In no event shall the School District be liable to the User for any damages whether direct, indirect, special or consequential, arising out the use of the Technology Systems or electronic devices. To the contrary, should a User incur charges, such charges will be the User's responsibility.

User Acknowledgement

The Board requires that each user and/or parent/guardian sign a document indicating their understanding of, agreement to, and intention to adhere to the terms of this policy.