File: IJNDB

ACCEPTABLE USE POLICY

1. Purpose

The purpose of the Acceptable Use Policy (AUP) is to establish the acceptable use of information technologies in the Wilmington Public Schools (WPS) in order to benefit the students, parents and staff of Wilmington and better our learning community. WPS encourages the use of information technology in our schools and the public at large. The District believes that the understanding and proper use of these technologies enhance learning and help our student population develop into productive and responsible citizens. Understanding information technologies can help to create lifelong learners who conduct themselves responsibly and ethically. These technologies will be used to increase efficiency, collaboration, communication, critical thinking and creativity.

2. General Statement of Policy

This policy will provide an explanation, purpose and definition of acceptable use by students, parents and staff of the WPS community. This policy is required to be read prior to using or accessing any information technology in the District. Additionally, staff must sign the (AUP) form and submit it to the WPS administrative office annually before accessing any information technology prior to the beginning of the new school year. Parents and students must check the box indicating that they have read this policy in the student handbook in the online student contact update form in the Aspen Parent Portal annually.

3. Implementation of this Policy

The Superintendent of Schools or his/her designee(s), shall develop and implement administrative regulations, procedures, terms and conditions for use and user agreements consistent with the purposes and mission of the WPS as well as with applicable laws and this policy. The review and update of this policy will be done annually by the Superintendent of Schools and the IT Director.

4. Definitions

Electronic Communication: Any communication or interaction which occurs through electronic means. Electronic communications include communications that have no specific intended recipient (e.g., posting a blog entry or status update on a publicly visible website, depending on privacy settings, which may be viewed by the public or users of that website).
Student: Any individual currently enrolled in the WPS.
The District: The Wilmington Public Schools and its staff.
The Committee: The Wilmington School Committee and its members.
Staff: All employees of the WPS and any contractor or individual employed by a contractor who provides services in or to the WPS.

Information Technology: The WPS Network Infrastructure, wireless network, hardware, software, systems, electronic devices, computers, peripherals, website, electronic documents and files, storage devices, data, Internet, digital resources, blogs, podcasting, telephone including Voice over Internet Protocol (VoIP), email or any other device or equipment used to access, store, manipulate or transmit data.
Users: Any person using the District's information technologies
Devices: Any District-owned or leased device, students or staff-owned device or any device being used on school grounds or on the school's network

5. Unacceptable Uses

a. Users will not use the District's electronic technologies to access, review, upload, download, store, print, post, receive, transmit or distribute:
   i. Pornographic, obscene or sexually explicit material or other visual depictions that are harmful to minors;
   ii. Obscene, abusive, profane, lewd, vulgar, rude, inflammatory, libelous, threatening, disrespectful, or sexually explicit language;
   iii. Materials that use language or images that are inappropriate in the educational setting or disruptive to the educational process;
   iv. Information or materials that could cause damage or danger of disruption to the educational process;
   v. Materials that use language or images that advocate violence or discrimination toward other people (hate literature) or that may constitute harassment or discrimination, or any other material that would violate any law.
   vi. Online shopping or ordering for personal purposes.
   vii. Personal photos, videos, files or music not related to educational purposes for any extended length of time with the exception of those stored in the apps provided by the District's Google Apps for Education
b. Users will not use the District's electronic technologies to knowingly or recklessly post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks.
c. Users will not use the District's electronic technologies to engage in any illegal act or violate any local, state or federal statute or law.
d. Users will not use the District's electronic technologies for political campaigning.
e. Users will not physically or electronically vandalize District technologies nor use the District's electronic technologies to vandalize, damage or disable the property of another person or organization.
   i. Users will not make deliberate attempts to degrade or disrupt equipment, software or system performance by spreading computer viruses or by any other means.
   ii. Users will not tamper with, modify or change the District's electronic technologies software, hardware or wiring or take any action to violate the District's security system.

iii. Users will not use the District's electronic technologies in such a way as to disrupt the use of the system by other users.

iv. Users may not add or remove any software from District-owned computers or devices nor modify the equipment, software configuration, or environment without prior expressed written permission from the Superintendent of Schools and/or his/her designee. [All electronic technology requests must go through the District's Office of Information Technology Work Order System.]

f. Users will not use the District's electronic technologies to gain unauthorized access (hacking) to information resources or to access another person's materials, information or files without the implied or direct permission of that person.

g. Users will not attempt to gain unauthorized access to the District's electronic technologies or any other system through the District's electronic technologies. Users will not attempt to logon through another person's account, or use computer accounts, access codes or network identification other than those assigned to the user. Access through any means other than an individual's user logon and password is not permitted.

h. Users will not use the District's electronic technologies to post information in public access areas regarding private information about another person. Private information includes personal contact information about themselves or other persons, or other personally identifiable information including, but not limited to, addresses, telephone numbers, identification numbers, account numbers, access codes or passwords, labeled photographs or other information that would make the individual's identity easily traceable, and will not repost a message that was sent to the user privately without permission of the person who sent the message.

i. Messages, files and records on the District's electronic technologies may not be encrypted in such a way that the Office of Information Technology cannot access them and without the permission of appropriate administrative school authorities.

j. Users will not use the District's electronic technologies in any way that may violate trademark or copyright laws or usage licensing agreements:

i. Users will not use another person's property without the person's prior approval or proper citation;

ii. Users will not load, download or exchange pirated software or copy software to or from any school computer including freeware and shareware;

iii. Users will not plagiarize works they find on the Internet or other information resources.

k. Users will not use the District's electronic technologies for unauthorized commercial purposes or for personal financial gain unrelated to the mission of the District. Users will not use the District's electronic technologies to offer or provide goods or services or for product advertisement, except as authorized by the District administration.

l. The District does not support personal hardware or software. Users will not install any personal hardware or software on any district-owned systems including but not limited to printers, wireless access points or switches. Users will not use district resources, Internet access or network via hardwire connection to the District network infrastructure. Users

will not connect their home PC or Laptop to the wall plate network jack in any building for Internet access.

m. Users will not use online proxy services to negate or otherwise bypass District Internet content filtering.
n. There are many people and systems dependent upon a proper and optimal performance level of the network infrastructure. Frivolous, excessive and inappropriate use of these network resources by one or a few individuals should not compromise the performance for other individuals and will operate with consideration for all who use the shared resources. The District may need to put quotas on storage or bandwidth as well as block websites or other online resources in order to maintain fairness of resource allocation for all district users.
o. Users are required to keep their passwords private and secured. Failure to do so could result in the unauthorized access of sensitive District data. Users who do not secure their passwords could have their access to systems, temporarily or permanently removed, or suspended and face disciplinary action. Examples of insecure storage of passwords include writing a password on a piece of paper attached to a monitor, under a keyboard, or pinned to a wall.

6. Children's Online Privacy Protection Act (COPPA)

Congress enacted the Children's Online Privacy Protection Act (COPPA) in 1998 (U.S.Code §6501, et seq. (COPPA) , 1998). COPPA required the Federal Trade Commission to issue and enforce regulations concerning children's online privacy. The Commission's original COPPA Rule became effective on April 21, 2000. The Commission issued an amended Rule on December 19, 2012 that became effective on July 1, 2013.

WPS works diligently to comply with COPPA requirements. WPS does not collect student personal information in order to transmit such information directly to online entities for the purpose of creating web-based accounts.

7. Public Records

The law requires public employees who send, receive or maintain records in their capacity as public employees, to retain, disclose and dispose of such records in compliance with strict provisions of the public records law (Massachusetts General Laws, Current). This law applies whether or not the record is in the form of a paper document or an electronic communication. When staff communicate through school-based resources, such as staff e-mail or school-sponsored web pages, such records are retained and archived through the school's information technology department. If, however, a teacher communicates outside of these resources, such information is not retained. The burden to comply with public records laws falls on the educator when using personal e-mail or social network accounts to communicate with students and/or parents and guardians on work-related issues.

8. Content Filtering

The WPS uses hardware and software designed to block access to certain sites and filter content as required by the Children's Internet Protection Act (CIPA) (U.S. Code, 2000). WPS is aware that not all inappropriate information can be filtered and the district will make an effort to correct any known gaps in the filtering of information without unduly inhibiting the educational use of age-appropriate content by staff and students. Users will inform teachers or administrators of any inadvertent access to inappropriate material, in order that there is appropriate modification of the filtering profile. WPS educates students about appropriate online behavior, including how to interact with other individuals with regard to ethics, safety, security, responsibility and sensitivity. WPS provides these educational opportunities as part of the WPS K-12 Information and Digital Literacy Goals and in line with the Massachusetts Technology Literacy Standards and Expectations (Massachusetts Department of Elementary and Secondary Education, 2008).

9. Monitoring and Limited Expectation of Privacy

By authorizing use of the School District electronic technologies, the District does not relinquish control over content or data transmitted or stored on the network or contained in files. Users should have no expectation of privacy in the contents of personal files on the District's electronic technologies.

p. The WPS monitors the use of the school department's network to protect the integrity and optimal operation of all computer and system networks.
q. The WPS will cooperate with copyright protection agencies investigating copyright infringement by users of the computer systems and network of the WPS.
r. Technicians and computer system administrators maintain full access rights to all storage devices, and may need to access/manage such storage devices as part of their duties.
s. Routine maintenance and monitoring of the system may lead to discovery that a user has or is violating the WPS Technology Acceptable Use Policy, other school committee policies, state laws, or federal laws.
t. Search of particular files of a user may be conducted at any time but shall ordinarily be the result of a reasonable suspicion that a user has violated the law or WPS Policies. In such circumstances, the investigation shall be conducted in order to determine the nature and extent of the alleged policy violation.
u. The District will cooperate fully with local, state and federal authorities in any investigation concerning or related to any illegal activities or activities not in compliance with School District policies conducted through the District's electronic technologies.

10. Limitation on School District Liability

Use of the District's educational technologies is at the user's own risk and is provided on an "as is, as available" basis. The District will not be responsible for any damage users may suffer, including, but not limited to, loss, damage or unavailability of data stored on the District's systems or for delays or changes in or interruptions of service, corruption in delivery or non-deliveries of information or materials, regardless of the cause. The District is not responsible for the accuracy or quality of any advice or information obtained through or stored on the District's

electronic technologies. The District will not be responsible for financial obligations arising through unauthorized use of the District's educational technologies or the Internet.

11. Violations of this Acceptable Use Policy

Violations of this policy may have disciplinary repercussions, including:

- Suspension of network, technology, or computer privileges
- Notification to parents
- Detention or suspension from school and school-related activities
- Legal action and/or prosecution
- Termination of employment for cause

Works Cited

Massachusetts Department of Elementary and Secondary Education. (2008, April 29). *http://www.doe.mass.edu/odl/student.html.* Retrieved from Massachusetts Department of Elementary and Secondary Education: http://www.doe.mass.edu/odl/standards/itstand.pdf
Massachusetts General Laws. (Current). Public Records Law G.L. Chapter 66. *Massachusetts General Laws*. MA, United States.
U.S. Code. (2000, December 21). Children's Internet Protection Act, 47 U.S.C. §254 (CIPA).
U.S.Code §6501, et seq. (COPPA) . (1998). Children's Online Privacy Protection Act, 15 U.S.C. §6501, et seq. (COPPA) .

Legal References

17 U.S.C. § 101 et. seq. (Copyrights)
15 U.S.C. § 6501 et. seq.
Children's Internet Protection Act of 2000 (CIPA) 47 U.S.C. § 254
47 C.F.R. § 54.520 (FCC rules implementing CIPA)
Title III of the Elementary and Secondary Education Act of 1965, 20 U.S.C. §1601, et seq., as amended.

Acknowledgements:

Burlington Public Schools Acceptable Use Policy. (2013, July) http://www.burlington.org/departments/schools/burlington_public_schools/docs/BPS_AUP_2013.pdf
Minnetonka, MN Public Schools Electronic Technologies Acceptable Use Policy (2012, May 3) https://www.minnetonka.k12.mn.us/policies/524.pdf
Longmeadow Public Schools Acceptable Use Policy Draft (2013, April 8) http://www.longmeadow.k12.ma.us/news/draftacceptableusepolicy
Triton Regional School District Acceptable Use Policy. (2014, April 30) http://www.trsd.net/wpfb-file/jre1048-acceptable-use-policy-agreement-pdf-4/

Revision adopted: September 23, 2015