

MEMORANDUM

TO: NWABSD Board of Education
Members

DATE: April 11, 2023

NUMBER: 23-087

FR: Office of the Superintendent

SUBJECT: Approval of Proposed
Revisions to BP 6146.4
Instruction, Internet and
District Technology; First
Reading

STRATEGIC PLAN/BOARD GOAL:

Improve Stakeholder Communication.

ABSTRACT:

Board policy revisions require Board approval.

ISSUE:

At issue is to approve the first reading of the proposed revisions to BP 6146.4 Instruction, Internet and District Technology and open for public comments.

BACKGROUND AND/OR PERTINENT INFORMATION:

The Superintendent/designee presents drafts or suggestions for board policy revisions when changes in law occur or when specific need occurs. Policy revisions shall normally be given two readings prior to adoption by the Board. This is the first reading of the proposed revisions to BP 6146.4 Instruction, Internet and District Technology. This revision was brought forward by Amy Eakin, Director of Technology and revisions require Board adoption. *Proposed changes are:* This update clarifies acceptable use of district technology.

The Board Policy Committee reviewed the proposed changes, recommends approval and to open for public comments.

ALTERNATIVES:

1. Approve the first reading to the proposed revisions to BP 6146.4 Instruction, Internet and District Technology as presented and open for public comments;
2. Do not approve first reading to the proposed revisions to BP 6146.4 as presented;
3. Take no final action.

ADMINISTRATION'S RECOMMENDATION:

The administration recommends the Board approve the first reading to the proposed revisions to BP 6146.4 Instruction, Internet and District Technology as presented and open for public comments.

BP 6161.4 INTERNET AND DISTRICT TECHNOLOGY

Note: *The following policy should be used by all districts providing student access to the Internet and other computer networks. An Internet safety policy is required for schools receiving universal service discounts.*

Note: *The Children’s Internet Protection Act requires school districts to adopt Internet safety policies as a condition of receiving technology funds under Title II, Part D of the No Child Left Behind Act ([20 U.S.C. § 6751-6777](#)) for the purpose of purchasing computers with Internet access or paying the direct costs associated with accessing the Internet. Additionally, districts must adopt an Internet safety policy to qualify for most federal universal service discounts ([47 U.S.C. § 254](#)).*

The district’s internet safety policy must include a “technology protection measure” that blocks or filters Internet access by both adults and minors to visual depictions that are obscene, child pornography, or with respect to use by minors, harmful to minors. As part of the funding application process, the district must certify that the required policy is in place and that the district is enforcing the use of these technology protection measures. The filter may be disabled by an administrator, supervisor, or other authorized person for “bona fide research or other lawful purpose.”

Effective July 1, 2012, the Internet safety policy must also include monitoring the online activities of minors when using district computers or networks. Further, the policy must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking sites and in chat rooms, and cyberbullying awareness and response.

As a condition of receiving universal service discounts, schools must also adopt and implement an Internet safety policy that addresses (1) 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 electronic communication; (3) unauthorized access (“hacking”) and other unlawful activities by minors online; (4) unauthorized disclosure, use, and dissemination of personal identification information regarding minors; and (5) measures designed to restrict minors’ access to harmful materials. Schools must hold at least one public hearing before adopting the policy. The types of materials considered inappropriate for minors will be determined by the local school board. Schools must make this policy available to the FCC upon request.

The Board recognizes the educational and communication opportunities that exposure to the Internet and other computer networks can provide students and staff. The Board intends that these technological resources provided by the district be used in a safe, responsible, and proper manner in support of the instructional program and for the advancement of student learning. The Board has established ~~the this~~ Internet and District Technology acceptable use policy to ensure appropriate use of ~~this these~~ resources. District technology includes, but is not limited to, District computers, laptops, tablets, and phones.

Authority

The Superintendent or designee shall notify students and parents/guardians about authorized uses of district technology and the Internet, user obligations and responsibilities, and consequences for unauthorized use and/or unlawful activities. This includes the following:

1. The electronic information available to students and staff does not imply endorsement of the content by the district, nor does the district guarantee the accuracy of the information received on the Internet. The district shall not be responsible for any information that may be lost, damaged, or unavailable when using the network, District technology, or for any information that is retrieved via the Internet.
2. The school district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet or District technology.
3. The use of District technology, the Internet and similar communication networks by students and staff is a privilege -- not a right. Failure to follow established rules can lead to appropriate disciplinary action as well as the loss of access to the Internet or other networks through school accounts. Legal action may be taken where/when appropriate.
4. School district computers, laptops, tablets, phones, and other District technologies are the property of the School District. At no time does the district relinquish its exclusive control of ~~computers~~ District technology provided for the convenience of the students and staff. ~~Computers~~ District technology shall may not be used to disseminate, maintain, or access sexually explicit, vulgar, indecent, offensive, or lewd communications, images, or videos. Nor may computers be used for harassment or bullying. District technology must be used in accordance with this policy.

(cf. 5131.43 Harassment, Intimidation and Bullying)

5. The School District reserves the right to inspect and review files and data on ~~district computers~~ District technology, and to monitor the online behavior of ~~minors~~ persons when using ~~district computers~~ District technology or networks. Such inspection and monitoring is for the purpose of ensuring compliance with laws and appropriate use of technology as specified in this and other policies. Monitoring may be conducted by school authorities when they deem it necessary, without notice, without ~~student~~ consent, and without a search warrant.

The Superintendent or designee shall ensure that all district computers with Internet access have a technology protection measure that blocks or filters Internet access to visual depictions that are (1) obscene, (2) child pornography, or (3) harmful or inappropriate to minors as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for adults only for bona fide research

or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator.

Internet Safety

To reinforce these measures, the Superintendent or designee shall implement measures to address the following:

1. Restricting student access to harmful or inappropriate matter on the Internet and World Wide Web;
2. Ensuring student safety and security of students and student information when using electronic communications;
3. Ensuring that students do not engage in unauthorized access, including "hacking," and other unlawful activities; and
4. Limiting unauthorized disclosure, use, and dissemination of personal identification information.

Note: *The Children's Internet Protection Act, defines "harmful to minors" as: ...any picture, image, graphic image file, or other visual depiction that – (A) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (B) 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 a lewd exhibition of the genitals; and (C) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.*

Use Guidelines

Internet access is limited to only those acceptable uses as detailed in this policy. Internet users may not engage in unacceptable uses.

1. School officials will develop a written permission slip for Internet use. This signed form must be on file prior to allowing students direct access to the Internet.
2. School officials must apply the same criterion of educational suitability used for other educational resources when providing access to Internet informational resources. The district will not allow school access for on-line games or any other areas determined to be non-education related.
3. Students and staff have the right to examine a broad range of opinions and ideas in the educational process, including the right to locate, use, and exchange information and ideas via all information formats including interactive electronic media and the Internet.
4. Users are responsible for the ethical and educational use of their own Internet accounts and District technology. These ~~accounts~~ are to be used only by the authorized owner of the account for the authorized purpose. Users shall not intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users on the network or on District technology. No

use of the network shall serve to disrupt the use of the network by others. Hardware and/or software shall not be destroyed, modified, or abused in any way.

5. Users have the responsibility to respect the privacy of other Internet users. The illegal installation of copyrighted software for use on district computers is prohibited.

5-6. District technology and networks shall may not be used to disseminate, maintain, or access sexually explicit, vulgar, indecent, offensive, or lewd communications, images, or videos. The District strictly enforces this provision.

6-7. Users are expected to display proper "netiquette" (network etiquette) at all times.

7-8. Staff members shall supervise students while students are using district Internet access to ensure that the students abide by these procedures. Users must follow all rules and regulations posted in the computer lab or other room where computers are in use. Users must follow the directions of the adult in charge of the computer lab or other room where computers are in use.

8-9. 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. Specifically, the following uses are prohibited:

- a. Use of the network or District technology to facilitate illegal activity.
- b. Use of the network or District technology for commercial or for-profit purposes.
- c. Use of the network or District technology for non-work or non-school related work, except in a de minimis fashion or as permitted elsewhere by Board Policy. during the school day.
- d. Use of the network or District technology for product advertisement or political lobbying.
- e. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
- f. Use of the network or District technology to access obscene or pornographic material.
- g. Use of inappropriate language or profanity on the network or District technology.
- g-h. Use of the network or District technology to engage in plagiarism.
- h-i. Use of the network or District technology to transmit material likely to be offensive or objectionable to recipients.
- i-j. Use of the network or District technology for hacking or intentionally obtaining, accessing, or modifying files, passwords, and data belonging to other users.
- j-k. Impersonation of another user, anonymity, and pseudonyms.
- k-l. Use of network facilities or District technology for fraudulent copying, communications, or modification of materials in violation of copyright laws.
- l-m. Loading or use of unauthorized games, programs, files, or other electronic media.
- m-n. Use of the network or District technology to disrupt the work of other users.
- n-o. Destruction, modification, or abuse of network hardware and software.

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

p-g. Invading the privacy of individuals, this includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature.

9-10. Loss of access and other disciplinary actions shall be consequences for inappropriate use. When appropriate, law enforcement agencies may be involved.

(cf. 6161.5 - Web Sites/Pages)

(cf. 6184 - Virtual/Online Courses)

Education

Note: *Effective July 1, 2012, the Children's Internet Protection Act requires that a school district's Internet safety policy provide for educating students about appropriate online behavior, including interacting with other individuals on social networking web sites and in chat rooms, as well as cyberbullying awareness and response.*

The Superintendent or designee shall provide age-appropriate instruction regarding safe and appropriate behavior on social networking sites, chat rooms, and other Internet services. Such instruction shall include, at a minimum, the dangers of posting personal information online, misrepresentation by online predators, how to report inappropriate or offensive content or threats, behaviors that constitute cyberbullying, and how to respond when subjected to cyberbullying.

(cf. 5131.43 Harassment, Intimidation and Bullying)

Note: *the following optional paragraph addresses access to social networking sites such as MySpace, Facebook, Xanga, Friendster, and others, and may be revised by districts that choose to allow limited access for educational purposes.*

Student use of district computers to access social networking sites is prohibited. To the extent possible, the Superintendent or designee shall block access to such sites on district computers with Internet access.

Policy Review

The district, with input from students and appropriate staff, shall regularly review and update this policy, the accompanying administrative regulation, and other relevant procedures to enhance the safety and security of students using the district's technological resources and to help ensure that the district adapts to changing technologies and circumstances.

Legal Reference:

UNITED STATES CODE

[15 U.S.C. 6501-6505](#) Children's Online Privacy Protection Act

[20 U.S.C. 6751-6777](#), Enhancing Education Through Technology Act, Title II, Part D

[47 U.S.C. § 254](#), Children's Internet Protection Act, as amended by the Broadband Data Improvement Act ([P.L. 110-385](#))

CODE OF FEDERAL REGULATIONS

[47 C.F.R. § 54.520](#), as updated by the Federal Communications Commission Order and Report 11-125 (2011)

Revised: ~~January 29, 2013~~ _____

Adopted: April 28, 2004

Northwest Arctic Borough School District