BP-6161.4 (a)

INTERNET

The Board recognizes the educational and communication opportunities that exposure to the internet and other computer networks can provide students and staff. The Bord 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 internet acceptable use policy to ensure appropriate use of this resource.

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 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.
3. The use of 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 and when appropriate.
4. School devices are the property of the School District. At no time does the district relinquish its exclusive control of computers provided for the convenience of students and staff. Computers shall not be used to disseminate sexually explicit, vulgar, indecent, offensive, or lewd communications. Nor may computers be used for harassment or bullying (refer to policy 5131.43, Harassment, Intimidation, and Bullying).
5. The School District reserves the right to inspect and review files and data on district computers, and to monitor the online behavior of students when using district computers 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, whithout student consent, and without a search warrant.

The Superintendent or designee shall ensure that all district devices 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.

INTERNET

An administrator, supervisor, or other authorized person may disable the filtering device for adults only for bona fide research or other lawful purpose, provide the person receives prior permission from the Superintendent or system administrator.

Use Guidelines

Internet access is limited to only those acceptable uses as detailed 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 online 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. These accounts are to be used only by the authorized owner of the account for the authorized purpose. User shall not intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users on the network. 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.
6. Users are expected to display proper "netiquette" (network etiquette) at all times.
7. Staff members shall supervise students while students are using district internet access to ensure that the students abide by these procedures. Users must follow the directions of the adult in charge of the room where computers are in use.
8. 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 to facilitate illegal activity
    b. Use of the network for commercial of for-profit purposes
    c. Substantial use of the network for non-work or non-school related work
    d. Use of the network for product advertisement or political lobbying
    e. Use of the network for hate mail, discriminatory remarks, offensive or inflammatory communication, harassment, or bullying
    f. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials
    g. Use of the network to access obscene or pornographic material
    h. Use of the network to transmit material likely to be offensive or objectional to recipients
        i. Unauthorized use of the network for hacking or intentionally obtaining, accessing, or modifying files, passwords, and data belonging to other users

INTERNET

j. Unauthorized impersonation of another user, anonymity, and pseudonyms
k. Use of network facilities for fraudulent copying, communications, or modification of materials in violation of copyright laws
l. Loading of or use of unauthorized games, programs, files, or other electronic media
m. Use of the network to disrupt the work of other users
n. Destruction, modification or abuse of network hardware and software
o. Quoting personal communications in a public forum without the original author's prior consent
p. Invading the privacy of individuals, this includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal nature

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

Internet Safety

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

1. Restricting access to harmful or inappropriate matter on the internet or 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.

Compliance with FTC Regulations and with the Children's Online Privacy Protection Act (COPPA) law

The COPPA law states that individuals under the age of 13 need to have specific privacy rights that protect their personal data from being collected and used for commercial purposes.

Wrangell Public Schools uses the Google "G-Suite for Education" family of apps as well as the Google SSO Service (Single Sign On) to log into external apps.

BP-6161.4 (d)

INTERNET

The use of G Suite in the classroom provides tools for students to create, collaborate, communicate, and develop the necessary critical thinking and technology skills in our world today. The access to these tools is entirely online and can be accessed 24/7 from any internet connected computing device or in an "off-line" mode if Wi-Fi access is not available.

These apps allow a user to sign into multiple programs without having to exit each program and begin separately. These programs are used at three of our physical locations (Evergreen Elementary, Stikine Middle School, and Wrangell High School). Access to Google services is set at the different schools via Student groups and have services that are appropriate at each school level.
Upon parent request accounts can be removed and students will be able to still log in to the school curriculums that are needed in the classroom (except for specific Google services, including Google Classroom) with individual accounts on each program.

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.

Student use of district computers to access social networking may be 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.

Note: An internet safety policy is required for schools receiving universal service discounts.

BP-6161.4 (e)

INTERNET

Note: The Children's Internet Protection Act requires school districts to adopt internet safety policies as a condition of receiving technology funds for the purpose of direct costs associated with accessing the internet. Additionally, district 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 minors, harmful to minors. As part of the funding application process, the district must certify that the required policy is in place and 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 the ability to monitor online activities of minors when using district computer or networks. Further, the policy must provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking sites, and 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.

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. § 51.520 as updated by the Federal Communications Order and Report

Adopted in Consultation with Legal Counsel:	January 14, 2002
Reviewed in Consultation with Legal Counsel:	June 10, 2011
Revised in Consultation with Legal Counsel:	August 8, 2011
Revised:	June 17, 2019
Revised:	December 13, 2021