

KENAI PENINSULA BOROUGH SCHOOL DISTRICT

148 North Binkley Street Soldotna, Alaska 99669-7553

Phone (907) 714-8888 Fax (907) 262-9132

www.kpbsd.k12.ak.us

SCHOOL BOARD COMMUNICATION

Title:	Policies Revision - Worksession		
Date:	October 27, 2011	Item Number:	Worksession
Administrator:	Dave Jones 		
Attachments:	BP 0530 Criteria for Closing Schools AR 4111 Recruitment and Selection BP 6145.2 Interscholastic Competition AR 6161.4 Acceptable Use Policy/Internet Safety Policy		

☐ Action Needed ☐ For Discussion ☐ Information ☒ Other: Worksession

BACKGROUND INFORMATION

The following policies and administrative regulations were reviewed by the Board Policy Committee on September 12, 2011. They are scheduled to be reviewed at the Board Worksession on November 8, 2011.

BP 0530 Criteria for Closing Schools... page 2

- Revisions to criteria for closing schools with enrollment counts of less than 10 students.

AR 4111 Recruitment and Selection... page 3

- Protocol for hiring a site level administrator has been added. Additionally, item #10 now spells out that the recommendation is forwarded to School Board "for contract approval (not assignment)."

BP 6245.2 Interscholastic Competition... page 5

- The District has consulted the attorney and has included "religion" as a basis of nondiscrimination in the second paragraph.

AR 6161.4 Acceptable Use Policy/Internet Safety Policy...page 6

- The AR has stated that "A copy of this policy is included in the KPBSD Parent/Student Handbook." The Handbook has been getting too long and this policy takes up about a third of the handbook. Due to recommendations from both school and parent groups to reduce the size, we have eliminated most of the text of the policy from the handbook; however, we still reference the policy number and provide a link on the online handbook.

ADMINISTRATIVE RECOMMENDATION

The administration recommends making these changes to policy.

CRITERIA FOR CLOSING SCHOOLS

Consideration will be given to closing and/or consolidating schools in the Kenai Peninsula Borough School District when declining enrollment reaches a point at which continued operation of all buildings would result in detrimental effects on a part or the District's entire educational program, and would result in adverse effects on the financial management of the District.

Considerations

1. Enrollment capacity – This consideration will include minimum needed enrollment for purposes of providing or scheduling effective, comprehensive educational programs.
2. Student displacement – This will include both the number of students involved and the severity of the effects of the displacement. Positive as well as negative effects will be considered.
3. Permanency of decision – This will include consideration of economic and demographic trends in the affected area.
4. Financial factors – This will include possible loss of revenue to the District as a result of closing, as well as potential savings for the District due to building maintenance and operation.

Criteria for Closing Schools Due to Enrollment of Less than Ten Students.

Once a school has fewer than ~~10-ten~~ students at the ~~official-enrollment-count date~~close of the twenty day count period, the school will be placed on a list of potential school closures for the following year. The Superintendent may recommend closure for the ~~next-current~~ year or may recommend the school stay in operation for ~~one-additional-the current~~ year. If a school has fewer than ~~10-ten~~ students for ~~two-consecutive-years~~one year, the school ~~will~~may be closed for the following school year.

Considerations

1. Permanency of decision – This will include consideration of enrollment projections and demographic trends.
2. Financial factors – Potential net savings will be determined as they relate to personnel, maintenance, and operating costs. Loss of separate site status and the accompanying loss of funding will also be considered.
3. Educational alternatives – This will include the location of the school in relation to other schools student might attend.

Kenai Peninsula Borough School District
Adoption Date: 04/03/06

RECRUITMENT AND SELECTION

The District shall employ the most qualified person available for each open position. The Superintendent shall develop recruitment and selection procedures which include:

1. Assessment of the District's needs to determine those areas where specific skills, knowledge and abilities are lacking.
2. Development of job descriptions which accurately portray the position.
3. Dissemination of vacancy announcements to ensure a wide range of candidates, when necessary.
4. Screening procedures which will identify the best possible candidates for interviews.
5. Interview procedures which will determine the best qualified candidate for hire.

The District will follow this process and protocol when hiring site level administration:

1. Administrator notifies superintendent that he/she will not be returning.
2. Communication plan is developed by superintendent and principal.
3. A meeting will be arranged with staff, site council, PTA, PTO, etc., and the public to gather information about characteristics and qualities for the administrative position.
4. Dates established for providing input to superintendent; each site is unique.
5. KPBSD administrators under contract for the following school year given consideration to transfer to the vacated position.
6. Criteria/priorities from school community reviewed against transfer requests –placement of current assistant principal or other KPBSD administration would happen at this time if viewed as a match.
7. Once an opening exists, Superintendent causes the position to be advertised.
8. Files reviewed, pre-screens occur by Human Resources/Superintendent.

Certificated Personnel

AR 4111(b)

RECRUITMENT AND SELECTION continued

9. Interviews are open to public – announced prior to interview date.
10. Recommendation is forwarded to School Board for contract approval (not assignment); if transfer situation after administrative contracts approved, change provided as informational item only.
11. Site Administrators with teaching responsibilities may be added to existing small school sites to increase the administrative allocation and reduce the teaching responsibilities at their current site.

There will be exceptions to this process in the event that site level administration notification is later than March 1. The process for assistant principal vacancies will be determined on a site-by-site basis.

~~All teachers hired on or after the first school day of the 2002-03 school year and working in a program supported with Title VII funds shall be highly qualified as defined by the No Child Left Behind Act, as well as state law. All teachers teaching in core academic subjects must be highly qualified by June 30, 2006 unless further time is permitted by law.~~ as defined by the No Child Left Behind Act.

Legal Reference

UNITED STATES CODE, TITLE 20

§ 1119 No Child Left Behind Act of 2001, P.L. 107-110

KENAI PENINSULA BOROUGH SCHOOL DISTRICT
Adoption Date: 08/01/2005

INTERSCHOLASTIC COMPETITION

The School Board considers the interscholastic program an integral component of the District educational program. The interscholastic program shall be geared to the interests and abilities of students of both sexes and varied in scope to ensure wide participation, consistent with the financial and personnel constraints of the District.

(cf. Student Interscholastic Handbook)
(cf. 6145 Cocurricular Activities)

The Board shall not approve membership of the District, or any school in the District, in any voluntary interscholastic athletic organization which discriminates against or denies the benefits of any program to any person on the basis of race, sex, religion or ethnic origin.

(cf. 0410 Nondiscrimination in District Programs and Activities)

The Board shall maintain general control over all aspects of the interscholastic athletic policies, programs and activities in the District, including eligibility, season of sport, number of sports, personnel, and sports facilities. The Superintendent shall be responsible to the Board for District compliance with federal and state laws.

The Board recognizes its responsibility to ensure that the health and welfare of students is given the highest consideration in planning a program of interscholastic competition. Special care shall be taken to ensure that all interscholastic training and competition is organized and supervised in a manner which will not overtax the physical capabilities of the participants. The District interscholastic program shall require for medical examinations, ongoing medical supervision, and the use of protective equipment as appropriate.

Legal Reference:

ALASKA STATUTES

14.18.040 Discrimination in recreational and athletic activities prohibited

ALASKA ADMINISTRATIVE CODE

4 AAC 06.115 Interscholastic activities 4 AAC 06.520 *Recreational and athletic activities*

4 AAC 06.600 Definitions

KENAI PENINSULA BOROUGH SCHOOL DISTRICT
Adoption Date: 8/10/09

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY**Terms and Conditions for Use****Purpose**

The Kenai Peninsula Borough School District provides all students access to computers, networks, and the Internet as a means to enhance their education. It is the intent to promote the use of computers in a manner that is responsible, legal, ethical, and appropriate. The purpose of this policy is to assure that all users recognize the limitations that are imposed on their use of these resources. Our many varied stakeholders work within a shared environment where all must follow the rules of use so as not to let their actions infringe on the opportunity of others to accomplish their work.

Electronic Related Technologies

Kenai Peninsula Borough School District Electronic Network Related Technologies is an interconnected system of computers, terminals, servers, databases, routers, hubs, switches, video-conferencing equipment, and wireless devices. The District's network is an inherent part of how we do business. The Acceptable Use Policy covers students, staff, and any other users accessing any part of the network. Files, data, emails and any other information stored on District-owned equipment or produced while working for the District, or while attending as a student, is the property of the District. Internet and email use is a privilege, not a right. A violation of the Acceptable Use Policy may result in termination of usage and/or appropriate discipline for both students and teachers.

Authorized Users

The District's computer network is intended for the use of authorized users only. This also applies to the District's Wi-Fi network. Authorized users include students, staff, and others with a legitimate educational purpose for access as determined by a Memorandum of Agreement with the District. Individual schools may grant guest access on a temporary basis, but only for bona-fide school-related business. Any person using the network, or using any devices attached to the network, agrees to abide by the terms and conditions set forth in AR 6161.4 District Acceptable Use Policy. ~~A copy of this~~This policy is ~~included in~~ referred to in the KPBSD Parent/Student Handbook.

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)**Assumption of Risk**

The District will make a good faith effort to keep the District network system in working order and its available information accurate. However, users acknowledge that there is no warranty or guarantee of any kind, either express or implied, regarding the accuracy, quality, or validity of any of the data or information residing on the District network or available from the Internet. The District has no ability to maintain such information and has no authority over these materials. For example, and without limitation, the District does not warrant that the District network will be error-free or free of computer viruses. In making use of these resources, users agree to release the District from all claims of any kind, including claims for direct or indirect, incidental, or consequential damages of any nature, arising from any use or inability to use the network, and from any claim for negligence in connection with the operation of the District network. Use of District computers and/or the District network is at the risk of the user.

Indemnification

The user indemnifies and holds the District harmless from any claims, including attorney's fees, resulting from the user's activities while utilizing the District network that cause direct or indirect damage to the user or third parties.

Other Electronic Devices

Other electronic devices include, but are not limited to, cellular telecommunication devices such as cellular phones, smart phones, pagers, text communication pagers, two-way text pagers, I-Pod Touches, and personal digital assistants. Any electronic device falls under the authority of the Acceptable Use Policy if used on school grounds regardless of whether they may or may not be wirelessly connected to the District network infrastructure. For example, texting or emailing inappropriate pictures to other students while at school would be a violation of the Acceptable Use Agreement even if only done using the user's personal cellular plan and using no District provided network services.

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)**Internet Non-Participation by Students**

Parents of minor students (under 18 years of age) may request that their student(s) not be allowed use of the Internet, by submitting E 6161.4 (a) Internet Access Non-Permission Form to the office at the student's school. This action will also deny access to the District wireless network.

Security

It shall be the responsibility of all members of the school staff to appropriately supervise and monitor usage to ensure compliance with this Acceptable Use Policy and the Children's Internet Protection Act. If a student inadvertently accesses inappropriate information, he or she should immediately disclose the inadvertent access to a teacher or to the school principal. All users are to promptly report any security violations of the Acceptable Use Policy to their teacher or the school principal. The principal should then report violations to Information Services. In order to maintain the security of the District network, users are prohibited from engaging in the following actions:

1. Using a modem to dial into any online service provider, or Internet Service Provider (ISP).
2. Attaching a wireless access point or any other network gateway to the District's network, thereby providing unsecured anonymous access to the District network.
3. Intentionally disrupting the use of any computer for other users, including, but not limited to, disruptive use of any processes or programs, intentionally spreading computer viruses, utilizing tools for ascertaining passwords, unauthorized use of a guest password, or engaging in "hacking" of any kind, which is an illegal or unlawful entry into an electronic system to gain secret unauthorized information.
4. Disclosing the contents or existence of District computer files, confidential documents, email correspondence, or other information to anyone other than authorized recipients.
5. Users must not use, or attempt to discover, the login or password belonging to someone else. Neither staff nor students should be using a guest account, but should always use the account provided to them by the District.
6. Unauthorized file sharing, downloading unauthorized games, programs, files, electronic media, and/or stand-alone applications from the Internet that may cause a threat to the District network is not permitted.

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)**Access to Wi-Fi**

Access to the wireless network by personally-owned computers, smart phones, or other devices is allowed by authorized users. The District must balance the needs to keep our network operational and protected from viruses or loss of service attacks with the educational advantages of a more open, inclusive network. With the wireless capability KPBSD has the ability to have an acceptable level of protection for our network and still allow computers into the wireless network. Exhibit 6161.4(b) KPBSD Wireless Information shows what service level can be expected from various computer operating systems. Most personally-owned computers or devices will connect to the wireless network; however, most will probably only connect at the Low-Speed Internet level. It is important to understand that access to network resources commonly taken for granted, like printer access, network file storage, and file backup are not likely available to the personally-owned computer user. Of particular note, the district does not provide data backups for data stored on a personally-owned device. Users are responsible for their own data and are cautioned to backup their own files in the event of a hard-drive or other failure on a personally-owned computer

Personally-owned equipment may NOT be attached to the network via an Ethernet cable or other wire. Wireless access by a personally-owned laptop is allowed but connecting to the physical network by plugging into a wall jack is never allowed.

Personally-owned Equipment

Schools not allowing students to bring personally-owned equipment to school are

- Kenai Youth Facility, and
- Spring Creek School.

Unless otherwise listed, students may bring laptops, netbooks, smart phones, personal digital assistants, etc. to school for their personal educational use. The user is responsible for assuring that personally-owned computers are ready for use with the District network. This includes assuring that user-loaded files and programs do not consume hard drive space needed for instructional or education requirements and needed software is loaded. The District will not troubleshoot or provide technical support on personally-owned equipment. Bringing personally-owned equipment to school is absolutely done

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)

at the users own risk. The District is not responsible for theft or damage of personal property, or any damage a user may suffer, including loss of data.

Caution: Because user-installed peer-to-peer networking takes place at home, perhaps to share music, staff should be aware that some of these services share ALL files on their computer. The user is responsible to safeguard the confidentiality of student-related data on a personally-owned computer.

Electronic Mail (Email)

Electronic Mail (email) consists of all electronically transmitted information including any combinations of text, graphics, audio, pictorial, or other information created on or received by a computer application system and includes the transmission data, message text, and all attachments.

The District provides two email addresses for staff (Microsoft Exchange/Outlook @ kpbsd.k12.ak.us and Google-Gmail @ g.kpbsd.org). The District provides one email address for grade 4-12 students (or lower grade at the request of the principal)--Google-Gmail @ g.kpbsd.org. The District does not filter email beyond the SPAM filtering done by Google for the District-provided Gmail email accounts. Google may also have rules for use beyond what is covered in this agreement. A parent has the option of not allowing their student access to the District-provided Gmail account. To opt out of the District-provided email, parents need to complete the [E 6161.4a Internet Access Non-Permission Form](#) and return to the school office. Such restriction, once signed, remains in force until rescinded by the parent or the legal age student.

Gmail is part of the Google Apps' online collaborative office productivity suite. Denying access to Gmail also denies access to Google Apps. Opting-out of Google Apps doesn't mean a student will not access email at school, it just means the District will not provide the email address for the student to use. There are many free email sites on the Internet that anyone can sign up for. Other free email sites are also not content filtered and may not filter SPAM.

SPAMMING, or the mass sending of email, from any District email accounts, for any purpose whatsoever, is strictly prohibited. Spammers often search out individuals and attempt to get people to divulge username or password information to allow the spammers to use an email account and our network to send out SPAM email. Users are prohibited from revealing network or email logon information to anyone. If an email account is compromised and used for these purposes, the account will be disabled.

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)

Users should not expect that their data, use of email, District computers, or the District network is private.

Blogs

The District also creates a personal web log or blog for each student and staff for educational use. The user must initially activate the blog. KPBSD blogs are only indexed within the District. However, if the address is shared, anyone on the Internet can view or contribute to the blog. Users are expected to maintain the same level of civility as required on all communication covered by this policy. Post with respect, stick to the facts, and avoid unnecessary or unproductive arguments.

Websites

The school's website is limited to school-related materials and events. Students may create web pages as a part of a class activity. The District has the right to exercise final editorial authority over the content and/or style of user web pages.

Monitoring

Network activity is logged by our Internet filter software including tracking of websites visited by users. Email processed, delivered, or stored on District-owned equipment is owned by the District and may be inspected by the District. Information Services uses software called VNC, to remotely access and control any District computer on the network, with or without the user's permission, but only for a legitimate purpose. Remote access, where the remote computer user grants permission for entry, has been given to some District-level support staff. Remote-access capability is commonly used to diagnose and quickly correct problems, or to train the remote staff member on some computer or software function.

Monitoring Staff Computer Usage

No member of KPBSD management has access to an employee's email accounts, web-browsing history, or data files. Information Services staff will provide such information to the Director, Human Resources, upon request.

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)**Monitoring Student Computer Usage**

School principals have access to student Gmail email accounts and to the Internet browsing history of the students at their school. Some principals may assign a designee for that access responsibility, such as assistant principals, counselors, or secretaries. Information Services has access to the above items, and also has access to a student's data files and will provide any of this information to a school principal or their designee upon request. Information Services staff will on occasion search logs for security violations and will report violators to the appropriate school principal or in some cases may take independent action.

Software

The Kenai Peninsula Borough School District will not install software that we are not licensed to use. There are no exceptions. All software license agreements and proof of ownership are documented in the Information Services department. Software is installed by Information Services staff or thorough tools provided by them to key school personnel. No commercial software will be installed on District-owned computers by other staff or students. If teachers buy software and want the software loaded on District computers, they will have to donate the software and license to the District and provide proof of purchase.

Home Use of District Owned Software – Staff Only

Some software publishers allow home use according to the "80/20 Rule." This rule states that if a school purchases a software license for a specific computer where the teacher/staff is the primary user (80%+ of the time), the teacher/staff may install the software on a home computer at no extra charge. The use of the software at home is governed by the same license agreement as at school, (i.e., it may not be used for commercial/for-profit use.) The 80/20 Rule only applies to staff as long as they are using the specific District computer (the staff's actual office/classroom computer) that has the software installed. If the software is removed from the specific District staff computer then the 80/20 rule is no longer in effect and the software must be removed from the home computer as well. Personally-owned laptops brought into the school setting are not covered under the intent of the 80/20 Rule. The 80/20 rule allows home use, but once the personally-owned laptop leaves home the 80/20 rule no longer applies. If a staff member leaves the employ of the School District 80/20 software must be removed from any home computer. Lab computers do not qualify for the 80/20 rule. Information Services will provide the software media to schools upon request. Schools can check out the media to staff to load the 80/20 software at home. It is the responsibility of the staff member to insure compliance with the 80/20 rule.

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)

Home use under the 80/20 Rule, or similarly-intended software licenses, are the only exception where District-owned software is allowed on personally-owned computers. The District does not buy Mac or Unix versions of software so it cannot provide those versions of software for home use under the 80/20 Rule.

Software on personally-owned laptops

Any staff or student bringing in their personally-owned computer to school must supply their own software. The District will not provide software for personally-owned computers used in schools.

I-pods or MP3 players. Only legally purchased music may be installed on a District-owned MP3 player or any district computer. It is the responsibility of the assigned I-Pod user to provide proof of ownership of all copyrighted music. The user must also backup their music as Information Services does not backup MP3 files nor check for MP3 files when imaging computers.

Lawsuits

The District will not defend users against lawsuit for Acceptable Use Policy violations including music, software, or print copyright violations.

User responsibilities

Users should be polite, kind, courteous, and respectful at all times. Users are expected to respect the property of others, including District property, and be responsible for using equipment appropriately, including using personally-owned equipment appropriately. The District's network is intended for educational use. Teachers and other staff should guide students in their computer use so that students will learn how Internet resources can provide valuable educational information from other classrooms, schools, national and international sources.

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)**The user should:**

1. Adhere to these guidelines each time the District network is used.
2. Use the resources available through the Internet and other electronic media to supplement material available through the classroom, media center or through any other resource provided by the school.
3. Make available for inspection by a principal or teacher upon request any messages or files sent or received at any District Internet location. Staff should have a legitimate safety concern to invoke inspection.
4. Show respect for the audience by using appropriate language. The use of ethnic slurs, personal insults, profanity, obscenities, or engagement in any conduct that would not be acceptable inside the school are prohibited.
5. Show proper consideration for topics that may be considered objectionable or inflammatory – for example - politics or religion.
6. Protect their own privacy. Be mindful that what is published on the Internet can be public for a long time.
7. Keep ALL personal information, including addresses, telephone numbers, and pictures of students or staff (or anyone else) confidential.
8. Re-post (to make appear online again) or forward emails only after obtaining the original author's prior consent. This is common courtesy.
9. Abide by all copyright and fair use laws, including print, music, and software copyright laws.
10. Report improper email messages to the teacher.
11. Use technology for school-related purposes during the instructional day.
12. Use these resources so as not to disrupt service to other users.

Unacceptable Uses. The user should:

1. Not use computers or the network inconsistent with or in violation of District or school rules.
2. Not use equipment for any illegal or unethical activity. This includes, but is not limited to, tampering with computer hardware or software, network equipment, unauthorized entry into computers, and vandalism or destruction of equipment, software, or computer data.
3. Avoid derogatory or inflammatory language that is generally considered offensive or threatening. The user should not use these resources to participate in "Cyber Bullying" such as personal attacks and/or threats to or against anyone.

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)

4. Not view or attempt to locate material (electronic, printed, audio, or video, that is unacceptable in a school setting) in any format. This includes, but is not limited to, sexist or racist material, sexually explicit, pornographic, obscene, or vulgar images or language; graphically-violent music, music videos, screen savers, backdrops, and pictures. The criteria for acceptability is demonstrated in the types of material made available to students by principals, teachers, and the school media center.
5. Not download, upload, import or view files or websites that purport the use of illegal drugs, alcohol or illegal and/or violent behavior except school-approved, teacher-supervised digital media.
6. Not plagiarize the work of others gained through use of the District network, or any other means.
7. Not use for soliciting or distributing information with the intent to incite violence; cause personal harm or bodily injury; or to harass, bully, or “stalk” another individual.
8. Not upload, post, email, transmit, or otherwise make available any content that is unlawful, dangerous, or may cause a security risk.
9. Not use for, but not limited to, wagering, gambling, junk mail, chain letters, jokes, raffles, or fundraisers.
10. Not use a District email account to express religious or political views.
11. Not play games, including Internet-based games, during the instructional day, unless school-approved and teacher-supervised.
12. Not use online social networks or any form of online publishing or online personal communication during the instructional day unless under the direction of a teacher.
13. Not use for financial gain or for the transaction of any personal business or commercial activities:
 - a. Including any activity that requires an exchange of money or use of a credit card number,
 - b. any purchase or sale of any kind,
 - c. or any use for product or service advertisement.
14. Not stream non-educational music or video during the instructional day.

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)

15. Not bypass or attempt to bypass the District's Internet filtering software. Use of proxy servers to bypass Internet filters or to conceal the identity of one's computer or user information on the network is prohibited.
16. Not deface or vandalize District-owned equipment in any way, or the equipment of another person, including but not limited to, marking, painting, drawing, marring, removing computer parts, or placing stickers on any surface.
17. Not intentionally seek information of, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent or assume the identity of others.
18. Not create or use unauthorized networks including, but not limited to voice, data, IP, peer to peer, or proxy networks.
19. Not download any programs, files, or games from the Internet or other sources that can be run or launched on the computer as a stand-alone program. These programs or files are sometimes called "executable files."
20. Not create direct links to inappropriate or illegal sites.
21. Not violate of any provision of the Family Educational Rights and Privacy Act which makes confidential a student's educational records, including, but not limited to, a student's grades and test scores.

The Children's Internet Protection Act (CIPA)

The Children's Internet Protection Act, enacted December 21, 2000 requires recipients of federal technology funds to comply with certain technology protection measures (Internet filtering) and policy requirements. Schools and libraries receiving funds for Internet access and/or internal connections services must also meet the Internet safety policies of the Neighborhood Children's Internet Protection Act (NCIPA) that addresses the broader issues of electronic messaging, disclosure of personal information of minors, and unlawful online activities. The Protecting Children in the 21st Century Act, enacted October 10, 2008, adds an additional Internet Safety Policy requirement covering the education of minors about appropriate online behavior.

Technology Protection Measure (Internet Filter)

Pursuant to the Children's Internet Protection Act (CIPA), the District uses filtering software, at this time M86 Security, to screen Internet sites for offensive material. The Internet is a collection of thousands of worldwide networks and organizations

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)

that contain millions of pages of information. Users are cautioned that many of these pages contain offensive, sexually explicit, and inappropriate material, including, but not limited to the following categories: adult content, nudity, sex, gambling, violence, weapons, hacking, personals/dating, lingerie/swimsuit, racism/hate, tasteless, and illegal/ questionable. In general, it is difficult to avoid at least some contact with this material while using the Internet. Even innocuous search requests may lead to sites with highly offensive content. Additionally, having an unfiltered email address on the Internet, as do both staff and students, may lead to receipt of unsolicited email containing offensive content. Users accessing the Internet do so at their own risk. No filtering software is one hundred percent effective, and it is possible that the software could fail. In the event that filtering is unsuccessful and users gain access to inappropriate and/or harmful material, the District will not be liable.

The District will never override the Internet filter for students and will only in the very rarest of circumstances override the filter, even for bona-fide research by adults. Requests for a filter override can be made by contacting Information Services.

Children's Internet Protection Act Definition of Terms:

Technology Protection Measure: The term "technology protection measure" means a specific technology that blocks or filters Internet access to visual depictions that are

- a. obscene, as that term is defined in section 1460 of title 18, United States Code;
- b. child pornography, as that term is defined in section 2256 of title 18, United States Code; or
- c. harmful to minors.

Harmful To Minors: The term "harmful to minors" means 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

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY (continued)

- c. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

Directory Information Parent Opt-out Form.

Parents of minor students (under 18 years of age) may request that the District not post their children's work, photographs or names on the Internet by completing and returning E5125.1(b) Directory Information Parent Opt Out Form to the school office.

Sanctions

The Terms and Conditions shall be used in conjunction with the District's discipline policies (AR5144). Individual schools may choose to have additional rules and regulations pertaining to the use of networked resources in their respective buildings. Failure to abide by this policy may subject the user to corrective action ranging from suspension of some or all access privileges up to and including expulsion, termination and prosecutions according to District Policies. Users may be denied access to the District network while an investigation is underway. If a user's access to the District network is suspended or revoked by network administrators as a result of violations of this policy, the user may appeal the suspension in writing, to the Superintendent within ten (10) days. If a violator is removed from the District network, there shall be no obligation to provide a subsequent opportunity to access the network.

Portions of this policy used with permission of Henrico County Public Schools.

*Legal Reference*CODE OF FEDERAL REGULATIONS

47CFR54.520-- Sec. 54.520 Children's Internet Protection Act

34CFR99—Part 99 Family Educational Rights & Privacy Act

UNITED STATES CODE

15 U.S.C. 6502-6505 Children's Online Privacy Protection Act

Title 18, Section 1460, Possession with intent to sell, and sale, of obscene matter

Title 18, Section 2256, Sexual Exploitation and Other Abuse of Children.

Title 17, Copyrights

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

Protecting Children in the 21st Century Act, October 10, 2008

KENAI PENINSULA BOROUGH SCHOOL DISTRICT

Adoption Date: ~~7/11/2011~~ _____