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:	**Administrative Regulations for Worksession and Approval**		
Date:	**May 21, 2012**	**Item Number:**	11c.
Administrator:	**Dave Jones, Assistant Superintendent**		
Attachments:	**AR 6161.4 Acceptable Use Policy/Internet Safety Policy with edits shown . . . . . 2** **AR 6161.4 Acceptable Use Policy/Internet Safety Policy with revisions incorporated . 22**		

[x] **Action Needed** [ ] **For Discussion** [ ] **Information** [ ] **Other:** _____

BACKGROUND INFORMATION

The attached AR 6161.4 Acceptable Use Policy/Internet Safety Policy was reviewed at the Policy Committee on May 7, 2012. It is presented here for both a Worksession and for approval at the Board meeting.

- The entire AR has been revised to meet the requirements of the Children's Internet Protection Act (as a condition of receiving technology funds under E-rate.)
- We are required as of July 1, 2012 to have this revised policy in place which includes monitoring the online activities of minors when using district computers and networks, educating minors about the appropriate online behavior, and cyberbullying awareness and response.
- Due to the July 1 deadline. We are requesting that this AR be fast-tracked through both the worksession and presented for approval at the Board meeting.

Note: Due to the substantial number of changes in the attached, we are including 1) a copy with the redline edits shown (red is edited; green is moved); and 2) a copy with revisions incorporated.

ADMINISTRATIVE RECOMMENDATION

The administration recommends the above changes for approval.

REVISIONS TO AR 6161.4

AASB Note: INTERNET
Effective July 1, 2012, the Children's Internet Protection Act regulations require that a district's Internet safety policy to include monitoring the online activities of minors when using district computers or networks. This has been added to the policy. Further, the policy must also provide for educating minors about appropriate online behavior, including social networking, chat rooms, and cyberbullying. This requirement was previously contained in the policy, although an "Education" heading has been added. Districts that are not yet providing instruction on Internet safety should be cognizant of the July 1, 2012 deadline.

The Legal Reference section and explanatory notes have been updated as well.

The AR, Security of Internet System, contains a minor language change.

The Exhibit (previously entitled Internet Access Permission Letter to Parents) has been replaced with a revised Student Internet User Agreement. The User Agreement was developed by the Anchorage School District.

The policy changes will require formal Board adoption.

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 federal laws require that the district's policy include operation and enforcement of~~ 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.

Instruction

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY AR 6161.4 (a)

Terms and Conditions for Use

General Information

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~~herein. This policy is ~~referred~~ referenced ~~to~~ in the KPBSD Parent/Student Handbook.

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.

Indemnification

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.~~

Ownership

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, are the property of the District.

Personally-owned ~~Equipment~~Electronic Devices

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

- ~~Kenai Youth Facility, and~~
- ~~Spring Creek School~~Marathon School.

Unless otherwise listed above, students may bring laptops, netbooks, smart phones, ~~personal digital assistants~~tablet computers, MP3 players, e-readers, 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 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.

~~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.~~ Wireless access by a personally-owned laptop is allowed, but connecting to the physical network by plugging into a wall jack is never allowed.

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~~ on school property would be a violation of the Acceptable Use ~~Agreement~~ Policy even if only done using the user's personal cellular plan and using no District provided network services.

Software on Personally-Owned Devices

The District will not provide software for personally-owned computers. Schools may distribute software apps to iPads, iPods, iPhones, or potentially other personally-owned (non-computer) devices, for both students and staff, if done in accordance with District policies in place at that time.

~~I-pods~~iPods 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~~iPod 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.

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 n~~Network resources commonly taken for granted, like printer access, network file storage, and file backup are not ~~likely~~ available ~~to~~for the personally-owned ~~computer user~~devices. ~~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.~~

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 one email address (@g.kpbsd.org) 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.

The District provides two email addresses for staff (Microsoft Exchange/Outlook @ kpbsd.k12.ak.us and Google-G~~m~~Mail @ g.kpbsd.org). Staff should use the Microsoft Exchange/Outlook @ kpbsd.k12.ak.us for all District communications.

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. Spammers have been surpisingly successful enticing staff to divulge network login information. ~~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.~~The District will never ask a user to disclose a username and password through an email. Any such request, regardless of how credible it may seem, is an attempt to hijack an account.

~~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, meaning they are not searchable from the Internet. However, if the URL address is shared, anyone on the Internet can view or

contribute to the blog. ~~U~~When using blogs, 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 created as part of a class activity.

Parental Request for Non-Participation by Students (Internet or Email Opt-Out)

Parents of minor students (under 18 years of age) may request that their student(s) not be allowed access to the Internet, or may opt out of District-provided Gmail email accounts by submitting *E 6161.4(a) Internet Access Non-Permission Form* to the office at the student's school. Such restriction, once signed, remains in force until rescinded by the parent or the legal aged student. This action also denies access to the District wireless network.

It should be noted that Gmail is part of the Google Apps online collaborative office productivity suite. Denying access to Gmail also denies access to Google Apps. Opting-out does not mean a student will not access email at school; it just means that the District will not provide the email address for the student to use. There are many free email sites on the Internet where anyone can get a free email account. Other free email sites are also not content filtered and may not filter SPAM.

~~**Non-Participation by Students**~~

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 *E 5125.1(b) Directory Information Parent Opt-Out Form* to the school office. ~~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**~~

No illegal entry (hacking) or unethical attempt should ever be made to access any network, computer, or data belonging to someone else. Users should never log on with the network credentials of another person, but should only use the username and password supplied by the District for their exclusive use. Users should make every effort to keep all passwords supplied by the District for their exclusive use secure and private. Any activity undertaken for the purpose of hiding one's identity, to bypass the Internet filter, or to spread computer viruses is forbidden. ~~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 the Information Services department. ~~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.~~

~~**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~~

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* 6161.4*a 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 commonly 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~~access, 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.

Monitoring Student Computer Usage

School principals have access to student Gmail 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 computer software that we are not licensed to use. There are no exceptions. All computer software license agreements and proof of ownership are documented in the Information Services department. Software is installed by Information Services staff or through tools provided by them to key school personnel. No commercial computer 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.~~

~~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**~~**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. It is the responsibility of all members of the school staff to appropriately supervise and monitor student usage to ensure compliance with this Acceptable Use Policy and the Children's Internet Protection Act. ~~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 Uses

It may be helpful to correlate acceptable behavior in the school building to what is acceptable behavior online. In the school setting, treat others as you would like to be treated. Show respect and kindness to others.

The User Should:

1. Adhere to ~~these~~ current Acceptable Use Policy 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.~~

2. ~~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.~~Immediately disclose an inadvertent access of inappropriate information to a teacher or the school principal.
~~4.~~3. Show proper consideration for topics that may be considered objectionable or inflammatory.
~~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.~~4. Keep ~~ALL~~ everyone's personal information confidential, including addresses, telephone numbers, and pictures~~ of students or staff (or anyone else) confidential.~~, etc.
~~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.~~5. Abide by all plagiarism, 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.~~
6. ~~Use these resources so as not to disrupt service to other users.~~Make available for inspection by a principal, or upon request by a teacher, any messages or files sent or received by a student at any District Internet location. Staff should have a legitimate safety concern to invoke inspection.
7. Use technology for school-related purposes during the instructional day.
8. Report any cyberbullying against any student to the principal.
~~12.~~9. Use Internet related Chat (IRC) or other instant messaging appropriately. Always know the person you are messaging.

Unacceptable Uses

Do not use derogatory or inflammatory language that is generally considered offensive or threatening. Do not insult, bully, threaten, or personally attack people. Be on your best school behavior while online.

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.~~

~~4.~~1. Not view or attempt to locate material in any format (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.~~2. Not download, upload, import or view files or websites that purport the use of illegal drugs, alcohol or illegal and/or violent behavior except when school-approved~~,~~ and teacher-supervised ~~digital media~~.

~~6. Not plagiarize the work of others gained through use of the District network, or any other means.~~

~~7.~~3. ~~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.~~4. ~~Not upload, post, email, transmit, or otherwise make available any content that is unlawful, dangerous, or may cause a security risk.~~

~~9.~~5. ~~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.~~6. ~~Not play games, including~~ Internet~~-based games, during the instructional day, unless school-approved and teacher-supervised.~~

7.

~~12.~~ Not use online social networks or any form of online publishing or online personal communication during the instructional day unless specifically allowed at school or under the direction of a teacher.

~~13.~~8. ~~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.~~9. Not stream non-educational music or video during the instructional day.

~~15.~~10. Not invade the privacy of individuals, including the unauthorized disclosure, dissemination, or use of information, photographs, or videos. ~~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.~~11. 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.

~~17.~~12. Not upload, post, email, transmit, create direct web links to, or otherwise make available any content that is inappropriate, unlawful, dangerous, or may cause a security risk.

~~18.~~13. Not use for~~, but not limited to,~~ wagering, gambling, junk mail, chain letters, jokes, raffles, or fundraisers.

14. Not use a USB storage device to launch software.

15. Not use a District email account to express religious or political views. When expressing personal opinions a personal account is to be used.

~~19.~~16. Not play games, including Internet-based games, during the instructional day, unless school-approved and teacher-supervised.

~~20.~~17. Not use for financial gain or for the transaction of any personal business or commercial activities~~:~~, including any personal purchase or sale activity that requires an exchange of money or use of a personal credit card number or for any product or service advertisement.

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.~~

~~21.~~18. Not waste school resources through improper or personal use of the computer system.

~~22.~~19. 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~~ in any way.

~~23. 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.~~

~~24. Not create or use unauthorized networks including, but not limited to voice, data, IP, peer to peer, or proxy networks.~~

~~25. 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."~~

~~26. Not create direct links to inappropriate or illegal sites.~~

~~27.~~20. 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. Staff members are solely responsible to safeguard the confidentiality of student-related data on a personally-owned computer.

Sanctions

Internet access 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. The Terms and Conditions shall be used in conjunction with the District's discipline policies (*AR 5144 Discipline).* 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.

The Children's Internet Protection Act (CIPA)

The Children's Internet Protection Act~~, enacted~~ was signed into law on December 21, 2000. To receive support for Internet access and internal connections services from the Universal Service Fund (USF), school and library authorities must certify that they are enforcing a policy of Internet safety that includes measures to block or filter Internet access for both minors and adults to certain visual depictions. The relevant authority with responsibility for administration of the eligible school or library must certify the status of its compliance for the purpose of CIPA in order to receive USF support. ~~requires recipients of federal technology funds to comply with certain technology protection measures (Internet filtering) and policy requirements.~~

~~Schools~~ In general, schools and ~~libraries~~ library authorities ~~receiving funds for Internet access and/or internal connections services~~ must ~~also~~ certify either that they have complied with the requirements of CIPA; that they are undertaking actions, including any necessary procurement procedures to comply with the requirements of CIPA; or that CIPA does not apply to them because they are receiving discounts for telecommunications services only. ~~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.~~

CIPA requirements include the following three items:

1. Internet Safety Policy

Schools and libraries receiving universal service discounts are required to adopt and enforce an Internet safety policy that includes a technology protection measure that protects against access by adults and minors to visual depictions

that are obscene, child pornography, or — with respect to use of computers with Internet access by minors — harmful to minors.

KPBSD Response: The Acceptable Use Policy/Internet Safety Policy addresses all required Internet Safety Policy issues.

Note: ~~In 2008, the Broadband Data Improvement Act amended the~~ Effective July 1, 2012, the Children's Internet Protection Act ~~to mandate~~ requires that a school district's Internet safety policy ~~now include~~ 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.

For schools, the policy must also include monitoring the online activities of minors. Note: beginning July 1, 2012, when schools certify their compliance with CIPA, they will also be certifying that their Internet safety policies have been updated to provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response.

KPBSD Response: Students will be provided 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)

2. Technology Protection Measure.

A technology protection measure is a specific technology that blocks or filters Internet access. The school or library must enforce the operation of the technology protection measure during the use of its computers with Internet access, although an administrator, supervisor, or other person authorized by the authority with responsibility for administration of the school or library may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose.

KPBSD Response: The District uses filtering software to screen Internet sites for offensive material. The Internet is a collection of thousands of worldwide networks and organizations 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.

3. Public Notice and Hearing or Meeting

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed technology protection measure and Internet safety policy. (For private schools, "public" notice means notice to their appropriate constituent group.) Unless required by local or state rules, an additional public notice and a hearing or meeting is not necessary for amendments to Internet safety policies.

KPBSD Response: Public notice and hearing are provided through the normal school board policy adoption process.

~~**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~~

~~**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

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 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

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)

~~*CODE OF FEDERAL REGULATIONS*~~
~~*47CFR54.520 - Sec. 54.520 Children's 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 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: 12/5/2011

REVISIONS INCORPORATED IN AR 6161.4

AASB Note: INTERNET
Effective July 1, 2012, the Children's Internet Protection Act regulations require that a district's Internet safety policy to include monitoring the online activities of minors when using district computers or networks. This has been added to the policy. Further, the policy must also provide for educating minors about appropriate online behavior, including social networking, chat rooms, and cyberbullying. This requirement was previously contained in the policy, although an "Education" heading has been added. Districts that are not yet providing instruction on Internet safety should be cognizant of the July 1, 2012 deadline.

The Legal Reference section and explanatory notes have been updated as well.

The AR, Security of Internet System, contains a minor language change.

The Exhibit (previously entitled Internet Access Permission Letter to Parents) has been replaced with a revised Student Internet User Agreement. The User Agreement was developed by the Anchorage School District.

The policy changes will require formal Board adoption.

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.

Instruction

ACCEPTABLE USE POLICY/INTERNET SAFETY POLICY AR 6161.4 (a)

Terms and Conditions for Use

General Information

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.

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 herein. This policy is referenced in the KPBSD Parent/Student Handbook.

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.

Indemnification

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.

Ownership

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, are the property of the District.

Personally-owned Electronic Devices

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

- Marathon School.

Unless otherwise listed above, students may bring laptops, netbooks, smart phones, tablet computers, MP3 players, e-readers, 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. The District will not troubleshoot or provide technical support on personally-owned equipment. Bringing personally-owned equipment to school is absolutely done at the users own risk. The District is not responsible for theft or damage of personal property including loss of data.

Wireless access by a personally-owned laptop is allowed, but connecting to the physical network by plugging into a wall jack is never allowed.

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 on school property would be a violation of the Acceptable Use Policy even if only done using the user's personal cellular plan and using no District provided network services.

Software on Personally-Owned Devices

The District will not provide software for personally-owned computers. Schools may distribute software apps to iPads, iPods, iPhones, or potentially other personally-owned (non-computer) devices, for both students and staff, if done in accordance with District policies in place at that time.

iPods 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 iPod 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.

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. Network resources commonly taken for granted, like printer access, network file storage, and file backup are not available for the personally-owned devices.

Electronic Mail (Email)

The District provides one email address (@g.kpbsd.org) for grade 4-12 students (or lower grade at the request of the principal). 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. The District provides two email addresses for staff (Microsoft Exchange/Outlook @ kpbsd.k12.ak.us and Google-GMail @ g.kpbsd.org). Staff should use the Microsoft Exchange/Outlook @ kpbsd.k12.ak.us for all District communications.

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. Spammers have been surpisingly successful enticing staff to divulge network login information. The District will never ask a user to disclose a username and password through an email. Any such request, regardless of how credible it may seem, is an attempt to hijack an account.

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, meaning they are not searchable from the Internet. However, if the URL address is shared, anyone on the Internet can view or contribute to the blog. When using blogs, 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 created as part of a class activity.

Parental Request for Non-Participation by Students (Internet or Email Opt-Out)

Parents of minor students (under 18 years of age) may request that their student(s) not be allowed access to the Internet, or may opt out of District-provided Gmail email accounts by submitting *E 6161.4(a) Internet Access Non-Permission Form* to the office at the student's school. Such restriction, once signed, remains in force until rescinded by the parent or the legal aged student. This action also denies access to the District wireless network.

It should be noted that Gmail is part of the Google Apps online collaborative office productivity suite. Denying access to Gmail also denies access to Google Apps. Opting-out does not mean a student will not access email at school; it just means that the District will not provide the email address for the student to use. There are many free email sites on the Internet where anyone can get a free email account. Other free email sites are also not content filtered and may not filter SPAM.

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 *E 5125.1(b) Directory Information Parent Opt-Out Form* to the school office.

Security

No illegal entry (hacking) or unethical attempt should ever be made to access any network, computer, or data belonging to someone else. Users should never log on with the network credentials of another person, but should only use the username and password supplied by the District for their exclusive use. Users should make every effort to keep all passwords supplied by the District for their exclusive use secure and private. Any activity undertaken for the purpose of hiding one's identity, to bypass the Internet filter, or to spread computer viruses is forbidden.

All users are to promptly report any security violations of the Acceptable Use Policy to the school principal. The principal should then report violations to the Information Services department.

Monitoring

Network activity is logged including websites visited by users. Email processed, delivered, or stored on District-owned equipment is owned by the District. Information Services commonly uses software 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 user grants permission for access, 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.

Monitoring Student Computer Usage

School principals have access to student Gmail 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 computer software that we are not licensed to use. There are no exceptions. All computer software license agreements and proof of ownership are documented in the Information Services department. Software is installed by Information Services staff or through tools provided by them to key school personnel. No commercial computer 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.

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. It is the responsibility of all members of the school staff to appropriately supervise and monitor student usage to ensure compliance with this Acceptable Use Policy and the Children's Internet Protection Act.

Acceptable Uses

It may be helpful to correlate acceptable behavior in the school building to what is acceptable behavior online. In the school setting, treat others as you would like to be treated. Show respect and kindness to others.

The User Should:

1. Adhere to current Acceptable Use Policy guidelines each time the District network is used.
2. Immediately disclose an inadvertent access of inappropriate information to a teacher or the school principal.
3. Show proper consideration for topics that may be considered objectionable or inflammatory.
4. Keep everyone's personal information confidential, including addresses, telephone numbers, and pictures, etc.
5. Abide by all plagiarism, copyright and fair use laws, including print, music, and software copyright laws.
6. Make available for inspection by a principal, or upon request by a teacher, any messages or files sent or received by a student at any District Internet location. Staff should have a legitimate safety concern to invoke inspection.
7. Use technology for school-related purposes during the instructional day.
8. Report any cyberbullying against any student to the principal.
9. Use Internet related Chat (IRC) or other instant messaging appropriately. Always know the person you are messaging.

Unacceptable Uses

Do not use derogatory or inflammatory language that is generally considered offensive or threatening. Do not insult, bully, threaten, or personally attack people. Be on your best school behavior while online.

The User Should:

1. Not view or attempt to locate material in any format (electronic, printed, audio, or video) that is unacceptable in a school setting. 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.

2. Not download, upload, import or view files or websites that purport the use of illegal drugs, alcohol or illegal and/or violent behavior except when school-approved and teacher-supervised.
3. Not use online social networks or any form of online publishing or online personal communication during the instructional day unless specifically allowed at school or under the direction of a teacher. Not stream non-educational music or video during the instructional day.
4. Not invade the privacy of individuals, including the unauthorized disclosure, dissemination, or use of information, photographs, or videos.
5. 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.
6. Not upload, post, email, transmit, create direct web links to, or otherwise make available any content that is inappropriate, unlawful, dangerous, or may cause a security risk.
7. Not use for wagering, gambling, junk mail, chain letters, jokes, raffles, or fundraisers.
8. Not use a USB storage device to launch software.
9. Not use a District email account to express religious or political views. When expressing personal opinions a personal account is to be used.
10. Not play games, including Internet-based games, during the instructional day, unless school-approved and teacher-supervised.
11. Not use for financial gain or for the transaction of any personal business or commercial activities, including any personal purchase or sale activity that requires an exchange of money or use of a personal credit card number or for any product or service advertisement.
12. Not waste school resources through improper or personal use of the computer system.
13. Not deface or vandalize District-owned equipment in any way, or the equipment of another person in any way.
14. 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. Staff members are solely responsible to safeguard the confidentiality of student-related data on a personally-owned computer.

Sanctions

Internet access 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. The Terms and Conditions shall be used in conjunction with the District's discipline policies (*AR 5144 Discipline).* Individual schools may choose to have additional rules and regulations pertaining to the use of networked resources in their respective buildings. 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.

The Children's Internet Protection Act (CIPA)

The Children's Internet Protection Act was signed into law on December 21, 2000. To receive support for Internet access and internal connections services from the Universal Service Fund (USF), school and library authorities must certify that they are enforcing a policy of Internet safety that includes measures to block or filter Internet access for both minors and adults to certain visual depictions. The relevant authority with responsibility for administration of the eligible school or library must certify the status of its compliance for the purpose of CIPA in order to receive USF support.

In general, schools and library authorities must certify either that they have complied with the requirements of CIPA; that they are undertaking actions, including any necessary procurement procedures to comply with the requirements of CIPA; or that CIPA does not apply to them because they are receiving discounts for telecommunications services only.

CIPA requirements include the following three items:

1. Internet Safety Policy

Schools and libraries receiving universal service discounts are required to adopt and enforce an Internet safety policy that includes a technology protection measure that protects against access by adults and minors to visual depictions that are obscene, child pornography, or — with respect to use of computers with Internet access by minors — harmful to minors.

KPBSD Response: The Acceptable Use Policy/Internet Safety Policy addresses all required Internet Safety Policy issues.

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.

For schools, the policy must also include monitoring the online activities of minors. Note: beginning July 1, 2012, when schools certify their compliance with CIPA, they will also be certifying that their Internet safety policies have been updated to provide for educating minors about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, cyberbullying awareness, and response.

KPBSD Response: Students will be provided 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)

2. Technology Protection Measure.

A technology protection measure is a specific technology that blocks or filters Internet access. The school or library must enforce the operation of the technology protection measure during the use of its computers with Internet access, although an administrator, supervisor, or other person authorized by the authority with responsibility for administration of the school or library may disable the technology protection measure during use by an adult to enable access for bona fide research or other lawful purpose.

KPBSD Response: The District uses filtering software to screen Internet sites for offensive material. The Internet is a collection of thousands of worldwide networks and organizations 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.

3. Public Notice and Hearing or Meeting

The authority with responsibility for administration of the school or library must provide reasonable public notice and hold at least one public hearing or meeting to address a proposed technology protection measure and Internet safety policy. (For private schools, “public” notice means notice to their appropriate constituent group.) Unless required by local or state rules, an additional public notice and a hearing or meeting is not necessary for amendments to Internet safety policies.

KPBSD Response: Public notice and hearing are provided through the normal school board policy adoption process.

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)

KENAI PENINSULA BOROUGH SCHOOL DISTRICT
Adoption Date: ~~12/5/2011~~_____