AR 6161.4
Acceptable Use Policy – Internet Safety Policy

Terms and Conditions for Use
General Information
Purpose

The Kenai Peninsula Borough School District provides all students and staff access to computers, networks, and the Internet as a means to enhance their education or carry out their job duties. 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~~ ensure 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

The Kenai Peninsula Borough School District ~~Electronic Network Related Technologies is~~maintains an interconnected system of computers, ~~terminals,~~ servers, databases, routers, ~~hubs,~~ switches, video-conferencing equipment, ~~and~~ wireless access points and related devices, building control, monitoring, and automation equipment, surveillance systems, and software platforms. Collectively, this arrangement of electronic equipment and software is referred to as the District network. The District~~'s~~ network is an ~~inherent~~ integral part of how we do business.

Authorized Users

The District~~'s computer~~ network is ~~intended~~ provided 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, or events covered by approved building use agreement(s). 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 accessed outside the District network and has no authority over these materials. ~~For example, and w~~Without limitation, the District does not warrant that the District network will be error-free ~~or~~, free of computer viruses, or meet specific Service Level Agreement (SLA) benchmarks such as uptime percentage. Reasonable efforts given available resources are made to ensure the District network remains highly-available to meet the needs and objectives of network users.

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

Content (~~F~~files, data, emails, or similar) ~~and any other information stored on District-owned equipment or~~ -produced while working for the District or while attending as a student using devices or connectivity provided by the District network remain~~, 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 or handheld devices (smart phones, tablets, or similar)~~, netbooks, smart phones, tablet computers, MP3 players, e-readers, etc.~~ to school for their personal educational use. The user is responsible for ~~assuring~~ ensuring 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~~connectivity for personally-owned ~~laptop~~ devices is ~~allowed~~provided to authorized users. Under no circumstances are personally-owned devices permitted to connect to the physical network via network cables or similar.~~, 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.

Individual schools and/or classrooms may have policies further restricting or defining periods of permitted use of personal equipment.

Software on Personally-Owned Devices

The District will not ~~provide~~ purchase software solely for use on personally-owned computers. Some software subscriptions maintained by the District for use on the District network may include provisions for installation by staff or students on personal devices and may be available for use during the period of time employed or attending the District. Installation of software on personally-owned devices remains the responsibility of the device owner. No support will be provided for software installed to personal devices. ~~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.~~

Files and Content

All files, including, but not limited to, images, audio recordings, digital music, videos, and software, obtained, stored, or accessed on the District network must adhere to and be used in accordance with federal copyright law.

Data Protection

The District makes a reasonable effort to maintain backups of content stored on the District network. No guarantees are made regarding performance or availability of backups. The District reserves the right to limit or otherwise define backup policies based on the type of data. For example, the District presently excludes digital music from backups.

~~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~~ denial 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 6161.4b 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.~~

Personal devices connected to the District wireless network are afforded internet connectivity, subject to filtering.

Network resources ~~commonly taken for granted~~available to district-managed devices, ~~like~~ such as printer access, network file storage, and file backups 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 are provided an account on the District email platform (Microsoft Exchange) under the email domain @kpbsd.k12.ak.us or @kpbsd.org, as well as a

Google Apps account under the email domain @g.kpbsd.org. Staff should use ~~the~~ Microsoft Exchange~~/Outlook @ kpbsd.k12.ak.us~~ as their primary email platform~~for all District communications~~.

Spamming / Unsolicited Email

~~SPAMMING~~Spamming, or the mass sending of unsolicited email, from any District email accounts, ~~for any purpose whatsoever~~in which the sender and recipient do not have an established business or educational relationship, 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 surprisingly 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.~~

Any legitimate mass-mailings in which the sender and recipient have an established business or educational relationship (such as sending a monthly school newsletter to parents of enrolled children, classroom announcements to parents of enrolled students, or similar) must honor requests from recipients to be removed from the mailing list. These requests must be processed in a timely fashion.

When sending a legitimate mass-mailing to recipients in multiple unrelated households, email addresses must be entered as Blind Carbon Copy (BCC) recipients to prevent personal email addresses from disclosure across households.

Account Security

It is the responsibility of the user to protect the credentials (username, password) for any account provided by KPBSD for an individual's exclusive use. Do not share your account credentials with anyone. Furthermore, the use of account(s) among multiple individuals without prior approval of KPBSD Information Services is prohibited.

Information Services staff, the District, or any agent acting on behalf of KPBSD will NEVER ask a user to disclose a username or password. Any such request, regardless of how credible it may seem, is an attempt to hijack an account and should be immediately reported to Information Services.

Any activities undertaken for the purpose of hiding one's identity, bypassing the internet filter, spreading computer viruses or malware, or attempts to access any network, computer, or data belonging to someone else, is forbidden. All users are to promptly report any known or suspected security violations or violations of the Acceptable Use Policy to the school principal. The school principal should then report these violations to Information Services for further review.

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 6161.4a 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 5125.1b 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. Secure Sockets Layer (SSL) technology or HTTPS web sites generally thought to be secure are commonly decrypted for certain websites and can be monitored. 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.~~
Upon request of the Director of Human Resources, designated Information Services staff may produce requested data associated with an employee. This data may include an employee's KPBSD Exchange, Google Apps, or Office 365 email, web browsing history, or other data stored on the District network.

Information Services employs a combination of automated and manual review of system logs, web browsing logs, wireless network access logs, and other logs generated as a result of using the District network for system performance monitoring, or indicators of security or policy violations. If a security or policy violation involving a staff member is detected through either automated or manual log reviews, Information Services will notify the Director of Human Resources. Information Services staff may take independent action to protect the integrity or security of the District network.

Monitoring Student Computer Usage

School principals have access to student computer files, ~~Gmail~~ Google Apps mail 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. Teachers also have access to computer files of the students in their classes. Information Services has access to the above items and will provide any of this information to a school principal their designee, or appropriate district office staff upon request. Information Services ~~staff will on occasion search logs~~employs a combination of automated and manual review of system logs, web browsing logs, wireless network access logs, and other logs generated as a result of using the District network for system performance monitoring, or indicators of security or policy violations. If a security or policy violation involving a student is detected through either automated or manual log reviews, Information Services ~~and~~ will report ~~violators~~ the violation to the appropriate school principal. ~~or in some cases may take independent action~~ Information Services staff may take independent action to protect the integrity or security of the District network.

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.

Information Services staff will not bypass system protection measures designed to ensure the continued and reliable operation of the District network. If a software product is not compatible with the District network as configured, such software shall not be used. Information Services is available to assist with determining compatibility prior to purchasing a software title.

Lawsuits

The District will not defend users against lawsuit for Acceptable Use Policy violations including music, video, 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. Practice exceptional digital citizenship, such as accessing materials or content relevant to instructional goals or objectives, managing an appropriate digital footprint, respecting copyright law, and protecting the privacy of others.
4. Show proper consideration for topics that may be considered objectionable or inflammatory.
5. Keep everyone's personal information confidential, including addresses, telephone numbers, and pictures, etc.
6. Abide by all plagiarism, copyright and fair use laws, including print, music, video, and software, and digital media copyright laws.
7. 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 location. Staff should have a legitimate safety concern to invoke inspection.
8. Use technology for school-related purposes during the instructional day.
9. Report any cyberbullying against any student to the principal.
10. Use Internet related Chat (IRC) or other instant messagingcollaboration tools (instant messaging, email, online forums, etc.) 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~~ 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~~ 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.

4.~~Not~~ NOT invade the privacy of individuals, including the unauthorized disclosure, dissemination, or use of information, photographs, or videos.

5.~~Not~~ 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~~ 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~~ NOT use for wagering, gambling, junk mail, chain letters, jokes, raffles, or fundraisers.

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

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

~~10~~9.~~Not~~ 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.

~~11~~10.~~Not~~ NOT waste school resources through improper or personal use of the computer system.

~~12~~11.~~Not~~ NOT deface or vandalize District-owned equipment in any way, or the equipment of another person in any way.

~~13~~12.~~Not~~ 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.

Additional Resources

Information Services maintains a knowledgebase of technical documentation and operating practices at https://support.kpbsd.org.

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.

   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.

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.