

## **District Internet Use Policies**

### **Table of Contents:**

#### **5000 Students**

- ❖ **BP 5139 Student Access To Networked Information Resources And Acceptable Use Philosophy .....2**
  - **AR 5139 Student Access To Networked Information Resources And Acceptable Use Philosophy .....4**
    - **E 5139 User Agreement And Parent Permission Form ..... 9**
    - **E 5139(b) KGBSD Network Services Code Of Conduct ..... 10**

#### **6000 Instruction**

- ❖ **BP 6161.4 Internet Acceptable Use Policy ..... 12**
  - **AR 6161.4 Security Of Internet System .....18**
    - **E 6161.4 Acceptable Use And Internet Access Permission Letter To Parents And Students .....20**

**STUDENT ACCESS TO NETWORKED INFORMATION RESOURCES AND ACCEPTABLE USE PHILOSOPHY**

**Background:**

As the use of telecommunication networks by students and educators increase, there is a need to clarify acceptable use and safety of those networks and to include federal regulations from the Children's Online Privacy Protection Act (COPPA) and the Children's Internet Protection Act (CIPA).

**Contents:**

Policy 5139 includes regulations for the safety and use of the Internet. It addresses acceptable use, privileges, accountability and responsibility, web publishing, network etiquette, reliability, security, safety, and vandalism.

**Purpose:**

Policy 5139 has been revised (1) to include the new federal regulations regarding issues of child safety and acceptable use of the Internet and (2) to be in compliance with Universal Service Fund for Schools and Libraries (E-rate) guidelines.

The Board recognizes that as telecommunications and other new technologies shift the way that information may be accessed, communicated and transferred by members of society, those changes may also alter instruction and student learning. The Board supports access by students to rich information resources along with the development by staff of appropriate skills to analyze and evaluate such resources.

Board Policy 6161.1 spells out principles of selection and requires that instructional and library materials support and enrich the curriculum while taking into account the varied instructional needs, learning styles, abilities and developmental levels of students. Telecommunications, electronic information sources and networked services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. In the past, instructional and library media materials could be selected based on the above criteria. Telecommunications, because it leads to any publicly available file server in the world, opens classrooms and libraries to electronic information resources which have not been screened by educators for use by students of various ages.

**STUDENT ACCESS TO NETWORKED INFORMATION RESOURCES AND ACCEPTABLE USE PHILOSOPHY**

Electronic information research skills are now fundamental to preparation of citizens and future employees in this Age of Information. The Board expects that staff will blend thoughtful use of such information throughout the curriculum and that the staff will provide guidance and instruction to students in the appropriate use of electronic resources. Staff will consult the guidelines for instructional materials contained in Board policy 6161.1 and will honor the goals set forth for selection of instructional materials.

Access to telecommunications will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people throughout the world. The Board believes that the benefits to students to electronic and telecommunication resources and collaboration, exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the Ketchikan Gateway Borough School District supports and respects each family's right to decide whether or not to apply for independent access.

**Acceptable Use**

Student Responsibilities

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior apply (see Board Regulation 5131 - Code of Conduct). The network is provided for students to conduct research and communicate with others. Access to network services will be provided to students who agree to act in a considerate and responsible manner.

Independent student use of telecommunications and electronic information resources will be permitted upon submission of permission forms by parents of minor students (under 18 years of age) and by students themselves. Many regional networks require agreement by users to acceptable use policies outlining standards for behavior and communication.

**KETCHIKAN GATEWAY BOROUGH SCHOOL DISTRICT  
Adoption Date: 7/10/02**

**STUDENT ACCESS TO NETWORKED INFORMATION RESOURCES AND ACCEPTABLE USE PHILOSOPHY**

**Procedures**

**1. Program Development**

In order to match electronic resources as closely as possible to the curriculum, district personnel will review and evaluate resources in order to offer “home pages” and menus of materials which comply with Board guidelines listed in Board Policy 6161.1 governing the selection of instructional materials. Staff will provide developmentally telecommunications and electronic information resources to conduct research and other studies related to the curriculum. All students will be informed by staff of their rights and responsibilities as users of the district network prior to gaining access, either as individual users or as a member of a class or group.

As much as possible, access to district information resources will be designed in ways which point students to those which have been reviewed and evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Students may pursue electronic research independent of staff supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferable and may not be shared.

**2. Internet Rules**

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior apply.

The Network is provided for students to conduct research and communicate with others. Independent access to network services is provided to students who agree to act in a considerate and responsible manner. Parent permission ID is required for minors. Access is a privilege, not a right. Access entails responsibility.

Individual users of the district computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with district standards and will honor the agreements they have signed.

**STUDENT ACCESS TO NETWORKED INFORMATION RESOURCES AND ACCEPTABLE USE PHILOSOPHY (continued)**

Network storage areas may be treated like school lockers. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on district servers will always be private.

During school, teachers of younger students will guide them toward appropriate materials. Outside of school, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

The following are not permitted:

- Sending or displaying offensive message or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using others' passwords
- Trespassing in others' folders, work files
- Intentionally wasting limited resources
- Employing the network for commercial purposes

**3. Technology Protection Measures**

The school district has installed filtering software or other technologies on all school computers with Internet access, and will enforce the operation of same during any use of those computers, to prevent minors from accessing visual depictions that are (1) obscene, (2) child pornography, or (3) harmful to minors.

The term "harmful to minors" is defined by the Communications Act of 1934 (47 USC Section 254 [h] [7]), as meaning any picture, graphic image file, or other visual depictions.

Filtering software is not foolproof. It diminishes the likelihood that searchers will inadvertently retrieve text or images that they may find offensive, but does not eliminate that possibility.

**STUDENT ACCESS TO NETWORKED INFORMATION RESOURCES  
AND ACCEPTABLE USE PHILOSOPHY (continued)**

Filters often block access to sites that users would consider both inoffensive and useful.

**4. Sanctions**

- a. Violations may result in a loss of access.
- b. Additional disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior.
- c. When applicable, law enforcement agencies may be involved.

**Internet and Electronic Mail Permission Form**

The Ketchikan Gateway Borough School District is pleased to offer students access to the district computer network for electronic mail and the Internet. To gain access to e-mail and the Internet, all students under the age of 18 must obtain parent or guardian permission and must sign and return this form to the library media specialists. Students 18 and over may sign their own forms.

Access to e-mail and the Internet will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with Internet users throughout the world. Families should be warned that some material accessible via the Internet may contain items that are illegal, defamatory, inaccurate or potentially offensive to some people. While our intent is to make Internet access available to further educational goals and objectives, students may find ways to access other materials as well. The district believes that the benefits to students from access to the Internet, in the form of information resources and opportunities for collaboration, exceed any disadvantages. Ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources. To that end, the Ketchikan Gateway Borough School District support and respect each family's right to decide whether or not to apply for access.

**District Internet and E-Mail Rules**

Students are responsible for good behavior on school networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior apply.

**STUDENT ACCESS TO NETWORKED INFORMATION RESOURCES  
AND ACCEPTABLE USE PHILOSOPHY (continued)**

The network is provided for students to conduct research and communicate with others. Access to network services is given to students who agree to act in a considerate and responsible manner. Parent or legal guardian permission is required. Access entails responsibility and is a privilege – not a right.

Individual users of the district computer networks are responsible for their behavior and communications over the networks. It is presumed that users will comply with district standards and will honor the agreements they have signed. Beyond the clarification of such standards, the district is not responsible for restricting, monitoring or controlling the communications of individuals utilizing the network.

Network storage areas may be treated like school lockers. Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on network servers will always be private.

Within reason, freedom of speech and access to information will be honored. During school, teachers of younger students will guide them toward appropriate materials. Outside of school, families bear the same responsibility for such guidance as they exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

As outlined in Board policy and regulations on students' rights and responsibilities, copies of which are available in school offices, the following are not permitted:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using others' passwords
- Trespassing in others' folders, work files
- Intentionally wasting limited resources
- Employing the network for commercial purposes

**Students**

AR 5139(e)

**STUDENT ACCESS TO NETWORKED INFORMATION RESOURCES  
AND ACCEPTABLE USE PHILOSOPHY (continued)**

Violations may result in a loss of access as well as other disciplinary or legal action.



**USER AGREEMENT AND PARENT PERMISSION FORM**

As a use of the Ketchikan Gateway Borough School District computer network, I hereby agree to comply with the above stated rules communicating over the network in a reliable fashion while honoring all relevant laws and restrictions.

Student Signature \_\_\_\_\_

As the parent or legal guardian of the minor student above, I grant permission for my son or daughter to access network computer services such as electronic mail and the Internet. I understand that individuals and families may be held liable for violations. I understand that some materials on the Internet may be objectionable, but I accept responsibility for guidance of Internet use – setting and conveying standards for my daughter of son to follow when selecting, sharing or exploring information and media.

Parent Signature \_\_\_\_\_

Name of Student \_\_\_\_\_

School \_\_\_\_\_ Grade \_\_\_\_\_

Soc. Sec.# \_\_\_\_\_ Birth Date \_\_\_\_\_

Street Address \_\_\_\_\_ Home Phone \_\_\_\_\_

## **KETCHIKAN GATEWAY BOROUGH SCHOOL DISTRICT NETWORK SERVICES CODE OF CONDUCT**

### **Definitions**

Network Services refers to the services provided on a local area network within a school, and a wide area network throughout the school district including Internet connectivity available from the desktops of computers on the network.

These services include:

- Access to word processing, spreadsheet, database, paint and draw multimedia presentation and other tools available on the network.
- Access to the school library catalog system at First City Libraries.
- Access to shared files and publications available on the wide area network.
- Access to Internet for information gathering, communications and publishing.

Network Users refers to students, staff and others given district network services.

### **Rights**

Users have the right to:

- Use available technology including network services in their daily learning.
- Examine a broad range of opinions and ideas in the educational process including the right to locate, use and exchange information and ideas using network services.
- Communicate with other individuals including those accessible using network services.

### **Responsibilities**

Users have the responsibility to:

- Use school district hardware and software competently and respectfully.
- Learn to use the network services needed.
- Monitor personal file space.
- Follow all state and federal statutes regarding copyright and technology use.
- Maintain and respect the privacy of personal account and activities.

**KETCHIKAN GATEWAY BOROUGH SCHOOL DISTRICT  
NETWORK SERVICES CODE OF CONDUCT**

Maintain and respect the privacy of the user accounts and activities of others.

Follow the established district guidelines for computer etiquette.

Report any violation to network services personnel.

**Unacceptable Uses**

Users may not:

Damage or disrupt equipment or system performance.

Corrupt the data of another user.

Waste resources such as paper, time or access for others.

Participate in malicious hacking such as gaining unauthorized access to resources.

Invade the privacy of others by activities such as eavesdropping or reading someone else's mail or files.

Use or publish information about an account owned by another user.

Use profanity, obscenity or other language which may be offensive to another user.

Post anonymous messages.

Use the network services for any illegal activity such as violation of copyright, plagiarism, or other contractual use agreements.

Allow obscene or disruptive materials to enter the district networks.

**INTERNET ACCEPTABLE USE POLICY**

The availability of vast amounts of data, while creating enormous learning opportunities for students, creates numerous liability risks for a district. These risks include suits by parents and students for inappropriate materials accessed via the computer network, as well as actions by computer software owners/services for unauthorized access and use of information by students, as well as by district staff. Finally, it is important that students are provided appropriate rules and directions regarding use of the Internet service.

Note: The Children’s Internet Protection Act took effect on April 20, 2001. The law requires school districts to adopt Internet safety policies as a condition of receiving funds under the Elementary and Secondary Education Act (20 U.S.C. § 7001) or universal service discounts under section 254 of the Communications Act of 1934 (47 U.S.C. § 254). Schools that receive funds under ESEA but do not receive universal service discounts must certify, as part of the application process, that they have in place an Internet safety policy which includes the use of filtering devices on computers with Internet access, thereby blocking entry to “visual depictions that are obscene or child pornography.” With respect to minors, the filter must also protect against access to materials that are “harmful to minors.” Schools must certify that they are also enforcing the use of these technology protection measures during any use of computers with Internet access, even those that are not accessible to the public. The filter may be disabled by an administrator, supervisor, or other authorized person for bona fide research or other lawful purpose.

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 materials on the Internet; (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 materials harmful to minors. Schools must hold at least one public hearing before adopting the policy. The types of materials considered inappropriate for minors will be determined by the local school board. Schools must make this policy available to the FCC upon request.

The Board recognizes the educational and communication opportunities that exposure to the Internet and other computer networks can provide students and staff. The Board provides access to the Internet as a means to improve the education for all of our students by taking students beyond traditional curriculum and learning activities to future-oriented curricula and problem-solving activities. The Board has established the Internet acceptable use policy to ensure appropriate use of this resource.

**INTERNET ACCEPTABLE USE POLICY** (continued)**Definition of the Internet**

The Internet is the major global network for education, research, public service, business and information interchange. The Internet is a collection of millions of interconnected computer networks around the world that make it possible to share information and educational resources. The networks are owned by commercial, research, governmental, and educational organizations, as well as by individuals.

**Authority**

1. The electronic information available to students and staff does not imply endorsement of the content by the district, nor does the district guarantee the accuracy of the information received on the Internet. The district shall not be responsible for any information that may be lost, damaged, or unavailable when using the network or for any information that is retrieved via the Internet.
2. The school district shall not be responsible for any unauthorized charges or fees resulting from access to the Internet.
3. The use of the Internet and similar communication networks by students and staff is a privilege -- not a right. Failure to follow established rules can lead to appropriate disciplinary action as well as the loss of access to the Internet or other networks through school accounts. Legal action may be taken where/when appropriate.
4. School computers and networks are the property of the School District. At no time does the district relinquish its exclusive control of computers networks, and network resources provided for the convenience of the students and staff.
5. Computers shall not be used to disseminate anything deemed harmful to minors as per the Children's Internet Protection Act (CIPA).
6. The School District reserves the right to inspect and review the files and system of any computer accessing the network or found on school grounds if it has reasonable cause to suspect that a user is using the computer for illicit or illegal purposes or for purposes in violation of this policy. Such inspection may be conducted by school authorities when they deem it necessary, without notice, without consent, and without a search warrant.

INTERNET ACCEPTABLE USE POLICY (CONTINUED)Internet Safety

Either the district network as a whole or each district computer with Internet access shall have a filtering device that blocks access to visual and non-visual depictions that are harmful or inappropriate to minors as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. The Superintendent or designee shall enforce the use of such filtering devices. An administrator, supervisor, or other authorized person may disable the filtering device for bona fide research or other lawful purpose, provided the person receives prior permission from the Superintendent or system administrator. The Superintendent or designee shall include measures in this policy's implementation plan to address the following:

1. Limiting student access to inappropriate matter as well as restricting access to harmful materials;
2. Student safety and security when using electronic communications;
3. Limiting unauthorized access, including "hacking" and other unlawful activities; and
4. Limiting unauthorized disclosure, use, and dissemination of personal identification information of the user or any person.

Note: The Children's Internet Protection Act, P.L. 106-554, defines "harmful to minors" as: ...any picture, image, graphic image file, or other visual depiction that – (A) taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion; (B) depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and (C) taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

## **INTERNET ACCEPTABLE USE POLICY** (continued)

### **Use Guidelines**

Internet access is limited to only those acceptable uses as detailed in this policy unless previously authorized to the District Superintendent or designee.

Internet users may not engage in unacceptable uses.

1. School officials will use a district-developed written permission slip for Internet use. This signed form must be on file prior to allowing students direct access to the Internet.
2. School officials must apply the same criterion of educational suitability used for other educational resources when providing access to Internet informational resources.
3. Students and staff have the right to examine a broad range of opinions and ideas in the educational process, including the right to locate, use, and exchange information and ideas via all information formats including interactive electronic media and the Internet.
4. Users are responsible for the ethical and educational use of their own Internet accounts. These accounts are to be used only by the authorized owner of the account for the authorized purpose. Access to any resources through an account other than your own is strictly prohibited. Users shall not intentionally seek information on, obtain copies of, or modify files, other data or passwords belonging to other users on the network. No use of the network shall serve to disrupt the use of the network by others. Hardware, software and/or resources shall not be destroyed, modified, abused in any way.
5. Users have the responsibility to respect the privacy of other Internet users. The illegal installation, use, or distribution of any copyrighted material, software, or media on district computers is prohibited.
6. Users are expected to display proper “netiquette” (network etiquette) at all times.
7. Staff members shall supervise students while students are using district property, network, and/or resources to ensure that the students abide by these procedures. Users must follow all rules and regulations posted in the

**INTERNET ACCEPTABLE USE POLICY** (continued)

computer lab or other room where computers are in use. Users must follow the directions of the authorized staff member supervising the computer lab or other room where computers are in use.

8. Students and staff are expected to act in a responsible, ethical, and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:
  - a. Use of the network to facilitate illegal activity.
  - b. Use of the network for commercial or for-profit purposes without prior consent of the district.
  - c. Use of the network for non-work or non-school related work.
  - d. Use of the network for product advertisement, political lobbying, or to forward political opinion.
  - e. Use of the network for bullying, hate mail, discriminatory remarks, and/or offensive or inflammatory communication.
  - f. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.
  - g. Use of the network to access obscene or pornographic material as defined by CIPA.
  - h. Use of inappropriate language or profanity on the network as defined by district policy.
  - i. Use of the network to transmit material likely to be offensive or objectionable to recipients.
  - j. Use of the network for hacking or intentionally obtaining, accessing, or modifying files, passwords, and data belonging to other users.
  - k. Impersonation of another user, anonymity, pseudonyms, and online handles.



**INTERNET ACCEPTABLE USE POLICY** (continued)

- l. Use of network facilities for fraudulent copying, communications, or modification of materials in violation of federal and state copyright laws.
  - m. Loading or use of unauthorized games, programs, files, or other electronic media.
  - n. Use of the network to disrupt the work of other users.
  - o. Destruction, modification, misuse or abuse of network hardware, software, and resources.
  - p. Quoting personal communications in a public forum without the original author's prior consent.
  - q. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information about anyone that is of a personal and/or private nature.
9. Loss of access and other disciplinary actions shall be consequences for inappropriate use. When appropriate, law enforcement agencies may be involved.

*(cf. 6161.5 - Web Sites/Pages)*  
*(cf. 6184 - Virtual/Online Courses)*

Legal Reference:

*CHILDREN'S INTERNET PROTECTION ACT, P.L. 106-554*  
*20 U.S.C. § 6801, et seq.*  
*47 U.S.C. § 254(h) and (l)*

*Revised 12/04*

**Instruction**

AR 6161.4(a)

**SECURITY OF INTERNET SYSTEM**

System security will be protected through the use of passwords based upon district security standards. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual.
2. Users are not to use a computer that has been logged in under another student's or teacher's name.
3. Any user identified as a security risk or having a history of problematic incidents may be denied access to the computers and network on the following terms.
  - a. First offense may result in a 2 week suspension.
  - b. Second offense may result in a 9 week suspension.
  - c. Third offense may result in a year long suspension.
4. An offense which threatens the safety or welfare of others or jeopardizes the network system may result in immediate suspension from all computer activities for a period of time determined by the District Superintendent.

**Safety**

To the greatest extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall immediately bring them to the attention of a teacher or administrator. A network user who engages in harassment or unwanted or unsolicited communication may be denied access to the computers and network on the following terms:

1. First offense may result in a 2 week suspension.
2. Second offense may result in a 9 week suspension.
3. Third offense may result in a year long suspension.
4. An offense which threatens the safety or welfare of others or jeopardizes the network system may result in immediate suspension from all computer activities for a period of time determined by the District Superintendent.

**SECURITY OF INTERNET SYSTEM** (continued)

Network users shall not reveal personal addresses or telephone numbers to other users on the network.

**Complaints**

Written complaints regarding student and/or staff access to or use of specific resources available on the Internet will be received, reviewed and acted upon in accordance with the district's policy on challenged instructional materials.

**ACCEPTABLE USE AND INTERNET ACCESS PERMISSION LETTER  
TO PARENTS AND STUDENTS**

The Ketchikan Gateway Borough School District schools have access to the Internet through its own network. This access is used for many academic purposes including, but not limited to, communication, research, and educational activities. Students will be allowed to access the Internet with teacher supervision.

Student safety on the Internet is an extremely important matter for the Ketchikan Gateway Borough School District. In addition to teacher supervision, the district protects children from harmful content available on the Internet by adhering to the requirements of the Children's Internet Protection Act, O.L. 106-554.

The Board may make changes to this form and to the policy when the law or common practice deems it necessary, or by the recommendation of the District Computer Technical Staff. The District will attempt to notify you of any such changes; however you can find the most up to date version of the acceptable use policy online at: [www.kgbsd.org](http://www.kgbsd.org); and following the following links: School Board/Board Policies/6000 Instruction/ BP 6161.4.

1. Students will abide by the policies and procedures of any networks to which they have access through the Internet.
2. Internet access is limited to only those acceptable uses as detailed in the district's Internet policy. Expectations of students using the school district's network include:
  - a. Applying the same privacy, ethical, and educational considerations used in other forms of communication
  - b. following directions of the adult in charge
  - c. respect of all copyright and license agreements
  - d. respect of other computer network users
  - e. proper citation of quotes, references, and sources
  - f. responsibility for any unauthorized charges or fees resulting from access to the Internet
  - g. responsibility for immediately notifying a teacher or administrator if he/she receives threatening or unwelcome communications.
3. Activities prohibited while on the school district's network include:
  - a. causing or contributing to the damage or modification of computer hardware, software, or data
  - b. intentionally wasting limited resources (such as bandwidth, time on a computer)
  - c. accessing, displaying, or sending written or graphic information which is obscene, inflammatory, derogatory, or offensive

**ACCEPTABLE USE AND INTERNET ACCESS PERMISSION LETTER  
TO PARENTS AND STUDENTS continued**

- d. accessing and/or using others' work, folders, files, or passwords without permission
- e. using the network for commercial purposes, financial gain, or fraud
- f. giving personal information of self or others (such as first and last name, physical address including street name and name of city or town, email address, phone number, social security number, and identifiable image) without a teacher's permission
- g. harassing, insulting, or attacking others
- h. facilitating illegal activity

Access to the computer network of the Ketchikan Gateway Borough School District is a privilege, not a right. Consequences for inappropriate use may include loss of computer access and/or other disciplinary actions. When appropriate, law enforcement agencies may be involved. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network on the following terms:

1. First offense may result in a 2-week suspension from all computer activities
2. Second offense may result in a 9-week suspension from all computer activities
3. Third offense may result in a year-long suspension from all computer activities
4. An offense which threatens the safety or welfare of others or jeopardizes the network system may result in immediate suspension from all computer activities for a period of time determined by the District Superintendent.

Network administrators may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on network servers will ever be private. The School District reserves the right to inspect and review computer files of any computer currently accessing the KGBSD computer network, either district-owned or personally-owned. Such inspection may be conducted by school authorities without notice, without student consent, and without a search warrant.

The district is not responsible for any information that may be lost, damaged, or unavailable while using the district's computer network.

**ACCEPTABLE USE AND INTERNET ACCESS PERMISSION LETTER  
TO PARENTS AND STUDENTS continued**

**PUBLISHING ON THE WORLD WIDE WEB**

Students enrolled in the Ketchikan Gateway Borough School District have exciting and enriching opportunities which take advantage of current technology in order to prepare them adequately for future opportunities. As part of your son's/daughter's educational program, (s)he will have the opportunity to publish documents and participate in projects on the World Wide Web. These documents might include, but are not limited to, their writing, artwork, collaborative projects with other students locally or internationally, individual projects or reports, group photographs of an activity or club, or an individual photograph.

In no case will a child's phone number or street address or box number be published. Neither will a document indicate a child's physical location other than attendance at a particular school or participation in school activities. Published documents will conform to school board policies. Additionally, documents to be published on the World Wide Web must be approved by a referring teacher before publication.