SCHOOL DISTRICT OF BAYFIELD

Rule-Internet Safety and Acceptable Use

A. Purpose

1. The District provides employees and students with access to the District's electronic communication system, which includes Internet access. Access to the District's computer and electronic communication systems by employees, students and others requires adherence to the District's Internet safety and acceptable use policy and rules, other District policies and state and federal laws and regulations.
2. The primary purpose of providing access is to enhance teaching and learning, thereby better preparing students for success in life and work. This access is provided to increase communication within the District, enhance productivity and assist users in improving their skills. Access is also provided to assist in the sharing of information with the local community, including parents/guardians, social service agencies, government agencies and businesses.
3. The District's electronic communication system shall primarily be used for school-related administrative and educational purposes. The system shall not be used for personal purposes during work hours.
4. The District's computer and electronic communication systems may not be used for commercial purposes, defined as purchasing or offering/providing goods or services.
5. District employees must recognize that electronic files and communications may be electronic records subject to state open records requirements, and they must take appropriate actions to maintain such records in compliance with state law.
6. The District makes no guarantees of any kind, either express or implied that the functions of the services provided by or through the District system will be error free or without defect. The District will not be responsible for any damage users may suffer, including but not limited to, loss of data or interruptions of service. The District is not responsible for the accuracy or quality of the information obtained through or stored on the system. The District will not be responsible for financial obligations arising through the unauthorized use of the system.

B. District Responsibilities

1. The District is responsible for teaching proper techniques and standards for participation, for guiding access to appropriate sections of the network, and for assuring that users understand consequences for misuse of the network. Particular concern include issues of privacy, copyright infringement, email etiquette and approved and intended use of all network resources.
2. Staff will actively monitor students who are engaged in online learning activities.
3. The District shall maintain an Internet filtering measure that blocks access to the three categories of visual depictions specified by the Children's Internet Protection Act – obscene material, child pornography, and material that is deemed harmful to minors. Other content may be blocked at the District's discretion. The District's Internet filtering measure may be relaxed or disabled fro bona fide research or other lawful purposes.

C. Access to the System

1. The District's acceptable use rules as outlined below govern all uses of the District network by students and staff.

2. All students and staff will be given the opportunity to access the network. Before access to the network is granted for District staff, a “Network User Agreement” form must be signed and on file with the District Technology Coordinator.
3. Students will be granted access to the District network and the Internet. If a parent/guardian does not want their child to use the Internet or District network resources they shall notify the District in writing of their desire.
4. A guest may receive an individual account with the approval of the District Technology Coordinator or the building administrator if there is a specific, District-related purpose requiring such access. Use of the system by a guest must be specifically limited to the District-related purpose.
5. Non-District owned hardware or software may not be introduced into the system without approval from the District Technology Coordinator or building administrators. A written request must be submitted to state the purpose for use of the hardware or software and the duration.

D. **Acceptable Use Rules**

1. **Personal Safety**

a. Students will not post personal contact information about themselves or other people on the network. Personal contact information includes, but is not limited to, address, telephone and work address.

b. Students will not agree to meet with someone they have met online without their parent’(s)/guardian'(s) approval and participation.

c. Users will promptly disclose to their teacher or other staff members present any messages they receive that are inappropriate or that make them feel uncomfortable.

2. **Unauthorized Activities**

a. Users will not attempt to gain unauthorized access to the District system or to any other computer system through the District system, or go beyond their authorized access. This includes attempting to log in through another person's account or access another person’s files.

b. Users will not install software on the local hard drive nor will they download executable files without prior approval from the site District Technology Coordinator. Users will not alter any software configuration that is stored on a workstation. Users may use media such as a 3.5" disk, a zip disk or a CD-R to transport data files that are being worked on at home and school.

c. Users will not make deliberate attempts to disrupt the computer system performance or destroy data by intentionally spreading computer viruses or by any other means.

d. Users will not use the District system to engage in any other illegal act, including, but not limited to, arranging for a drug sale or the purchase of alcohol, engaging in criminal gang activity, utilizing packet capture programs, or threatening the safety of another person.

e. Users will not use the District’s network for personal gain or commercial purposes.

3. System Security

a. Users are responsible for the use of their individual accounts and should take all reasonable precautions to prevent others from being able to use their personal accounts. Under no conditions should a user provide his/her password to another person.

b. Users will immediately notify the District Technology Coordinator if they have identified a possible security problem. Users will not search for security problems because this may be construed as an unauthorized attempt to gain access, i.e. computer hacking.

C. Users will log off or lock their system when not using the resource or when it is not in direct view of the user.

4. **Inappropriate Language/Respect for Privacy**

a. Restrictions against inappropriate language apply to public messages, private messages and material posted on web pages.

b. Users will not use obscene, profane, lewd, vulgar, rude, inflammatory, threatening or disrespectful language.

c. Users will not post information that, if acted upon, could cause damage, danger or disruption.

d. Users will not engage in personal attacks, including prejudicial or discriminatory attacks.

e. Users will not harass another person. Harassment is persistently acting in a manner that distresses or annoys another person. If a user is told by a person to stop sending him/her messages, he/she must stop.

f. Users will not knowingly or recklessly post false or defamatory information about a person or organization.

g. Users will use discretion when forwarding a message that was sent to them privately without permission of the person who sent them the message.

5. **Respecting Resource Limits**

a. Staff will use the system primarily for educational, professional or career development activities. Students will use the system for educational activities. Any other student uses must be approved by District staff.

b. Students may download files only with a staff member's permission.

c. Users will not post chain letters or engage in "spamming." Spamming is sending an annoying or unnecessary message to a large number of people.

d. Staff are required to check their District email daily and delete unwanted messages promptly. Email messages are to be retained only as long as they serve their purpose and then should be deleted. Further, users need to delete unnecessary files in home and/or shared folders.

e. Users will not engage in activity that would disrupt or diminish the access to network resources by others.

6. **Plagiarism and Copyright Infringement**

a. Users will not plagiarize. Plagiarism is taking the works of others and presenting them as if they were original to the user. District policies on plagiarism will govern use of material accessed through the District system. Teachers will instruct student in appropriate research and citation practices.

b. Users will respect the rights of copyright owners. Copyright infringement occurs when an individual inappropriately reproduces a work that is protected by a copyright. If a work contains language that specifies acceptable use of that work, the user should follow the expressed requirements. If the user is unsure whether or not he/she can use a work, he/she should request permission from the copyright owner and appropriately reference it. District policies on copyright govern the use of material accessed through the District system. Because the extent of copyright protection of certain works found on the Internet is unclear, employees will make a standard practice of requesting permission from the holder of the work if their use of the material has the potential of being considered an infringement. Teachers will instruct students to respect copyright and to request permission when appropriate.

7. **Inappropriate Access to Material**

a. Users will not use the District system to access material that is profane or obscene (i.e., pornography), that advocates illegal acts, or that advocates violence or discrimination towards other people (hate literature).

b. If a user inadvertently accesses such information, he/she should immediately disclose the inadvertent access in a manner specified by his/her teacher. This will protect users against an allegation that they have intentionally violated the District's Internet safety and acceptable use policy or rules.

E. Search and Seizure

1. System users have a limited privacy expectation of the contents of their personal files on the District system. Emails and documents that reside on District resources are property of the District.
2. A search of a user's documents and email may be done at any time by District administration.
3. Internet usage is tracked by user and inappropriate or excessive use will be reported to the users supervisor or Building principal.

CROSS REFERENCE:	361.1	Copyright
	385	Internet Safety and Acceptable Use
	385 Exhibit 1	Staff Acceptable Use for Network Resources
	385 Exhibit 2	Student Acceptable Use for Network Resources
	385 Exhibit 3	Student Opt-out Form for Network Resources
	385 Exhibit 4	Request to Use Personal Electronic Device
	445.1	Locker Searches
	445.2	Search of Students and Student

APPROVED: June 9, 2008