West Bonner County School District

STUDENTS **3270P**

Acceptable Use of Electronic Networks

All use of electronic networks shall be consistent with the District's goal of promoting educational excellence by facilitating resource sharing, innovation, and communication. These procedures do not attempt to state all required or proscribed behaviors by users. However, some specific examples are provided. **The failure of any user to follow these procedures will result in the loss of privileges, disciplinary action, and/or appropriate legal action.**

Terms and Conditions

1. Personal use of computers by students that is consistent with the District's educational mission may be permitted during class when authorized by the teacher. Personal use of District computers and networks outside of class must comply with District policy.

2. Privileges – The use of the District's electronic networks is a privilege, not a right, and inappropriate use will result in a cancellation of those privileges. The system administrator (and/or building principal and/or Internet Safety Coordinator) will make all decisions regarding whether or not a user has violated these procedures, and may deny, revoke, or suspend access at any time. His or her decision is final.

3. Unacceptable Use – The user is responsible for his or her actions and activities involving the network. Some examples of unacceptable uses are:

    a. Using the network for any illegal activity, or to access websites encouraging illegal activity including violation of copyright or other contracts, or transmitting any material in violation of any U.S. or state law;

    b. Accessing information pertaining to the manufacture of weapons;

    c. Uses that cause harm to others or damage property;

    d. Unauthorized downloading of software, regardless of whether it is copyrighted or devirused;

    e. Downloading copyrighted material;

    f. Using the network for private financial or commercial activities;

    g. Wastefully using resources, such as file space;

    h. Hacking or gaining unauthorized access to files, resources, or entities; uploading a worm, virus, or other harmful form of programming;

i. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information of a personal nature about anyone;

j. Using another user's account or password or some other identifier that misleads message recipients into believing that someone other than you is communicating;

k. Posting material authored or created by another, without his/her consent;

l. Posting anonymous messages;

m. Using the network for commercial or private advertising;

n. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, nudity or near nudity, profane, sexually oriented, threatening, racially offensive, harassing, bullying or illegal material;

o. Using the network while access privileges are suspended or revoked;

p. Promotion of political, personal, or religious causes in a way that presents such opinions as the view of the District;

q. Disclosure identifying personal information or arranging to meet persons met on the internet or by electronic communications;

r. Any other unacceptable uses as outlined in District Policy 3270.

4. Network Etiquette – The user is expected to abide by the generally accepted rules of network etiquette. These include, but are not limited to, the following:

a. Be polite. Do not become abusive in messages to others.

b. Use appropriate language. Do not swear or use vulgarities or any other inappropriate language.

c. Do not reveal personal information, including the addresses or telephone numbers, of students or staff.

d. Recognize that electronic mail (e-mail) is not private. People who operate the system have access to all mail. Messages relating to or in support of illegal activities may be reported to the authorities.

e. Do not use the network in any way that would disrupt its use by other users.

f. Consider all communications and information accessible via the network to be private property of The District.

5. No Warranties – The District makes no warranties of any kind, whether expressed or implied, for the service it is providing. The District will not be responsible for any damages the user suffers. This includes loss of data resulting from delays, non-deliveries, missed deliveries, or service interruptions caused by its negligence or the user's errors or omissions. Use of any information obtained via the Internet is at the user's own risk. The District specifically denies any responsibility for the accuracy or quality of information obtained through its services.

6. Indemnification – The user agrees to indemnify the District for any losses, costs, or damages, including reasonable attorney fees, incurred by the District, relating to or arising out of any violation of these procedures.

7. Security – Network security is a high priority. If the user can identify a security problem on the Internet, the user **must** notify the system administrator, Internet Safety Coordinator and/or building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account. Attempts to log on to the Internet as a system administrator will result in cancellation of user privileges. Any user identified as a security risk may be denied access to the network.

8. Vandalism – Vandalism will result in cancellation of privileges, and other disciplinary action. Vandalism is defined as any malicious attempt to harm or destroy data of another user, the Internet, hardware, software, or any other network. This includes, but is not limited to, the uploading or creation of computer viruses.

9. Telephone Charges – The District assumes no responsibility for any unauthorized charges or fees, including telephone charges, long-distance charges, per-minute surcharges, and/or equipment or line costs.

10. Copyright Web Publishing Rules – Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Websites or file servers, without explicit written permission.

    a. For each republication (on a Website or file server) of a graphic or text file that was produced externally, there must be a notice at the bottom of the page crediting the original producer and noting how and when permission was granted. If possible, the notice should also include the Web address of the original source.

    b. Students engaged in producing Web pages must provide the webmaster with e-mail or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.

    c. The absence of a copyright notice may not be interpreted as permission to copy the materials. Only the copyright owner may provide the permission. The manager of the Website displaying the material may not be considered a source of permission.

d. The “fair use” rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.

e. Student work may only be published if there is written permission from both the parent/guardian and the student.

f. Violation of the copyright web publishing rules may result in denial of access to the network.

11. Use of Electronic Mail.

a. The District’s electronic mail system, and its constituent software, hardware, and data files, are owned and controlled by the District. The District provides e-mail to aid students in fulfilling their duties and responsibilities and as an education tool.

b. Email could be subject to public records requests and disclosures depending upon the subject matter of the contents of the email. Student email accounts will have an “In Place Hold” for three (3) months. An in place hold will preserve items for a specific duration of time (3 months).

c. The District reserves the right to access and disclose the contents of any account on its system, without prior notice or permission from the account’s user. Unauthorized access by any student to an electronic mail account is strictly prohibited.

d. Each person should use the same degree of care in drafting an electronic mail message as would be put into a written memorandum or document. Nothing should be transmitted in an e-mail message that would be inappropriate in a letter or memorandum.

e. Electronic messages transmitted via the District’s Internet gateway carry with them an identification of the user’s Internet “domain.” This domain name is a registered domain name and identifies the author as being with the District. Great care should be taken, therefore, in the composition of such messages and how such messages might reflect on the name and reputation of this District. Users will be held personally responsible for the content of any and all electronic mail messages transmitted to external recipients.

f. Any message received from an unknown sender via the Internet should either be immediately deleted. Downloading any file attached to any Internet-based message is prohibited, unless the user is certain of that message’s authenticity and the nature of the file so transmitted.

g. Use of the District’s electronic mail system constitutes consent to these regulations.

<u>Internet Safety</u>

1. Internet access is limited to only those "acceptable uses," as detailed in these procedures. Internet safety is almost assured if users will not engage in "unacceptable uses," as detailed in District policy and procedures, and will otherwise follow District policy and procedures.

2. Staff members shall supervise students while students are using District Internet access at school, to ensure that the students abide by the Terms and Conditions for Internet access, as contained in these procedures.

3. Each District computer with Internet access has a filtering device that blocks entry to visual depictions that are: (1) obscene; (2) pornographic; or (3) harmful or inappropriate for students, as defined by the Children's Internet Protection Act and as determined by the Superintendent or designee. Student's must use the District's filtered network for all online activities on school grounds or using District equipment.

4. The system administrator, Internet Safety Coordinator and/or building principals shall monitor student Internet access.

Student Use of Social Media

Students will be held accountable for the content of the communications that they post on social media locations and are responsible for complying with District policy and procedures for content posted using a District computer, network, or software and /or when posted during school hours when the student is in attendance at school. Student posts on social media locations outside of school hours and school grounds using a personal computer, network, and software shall be private as long as they do not enter into the educational setting and interfere wit the orderly operation of the school. Posts to social network sites using a District computer, network or software may be subject to public records requests. Students may not disrupt the learning atmosphere, educational programs, school activities, and/or rights of others.

All of the requirements and prohibitions in District policy and procedure apply to the use of social media on school grounds, through the District network or using District equipment, or as part of a class assignment.

Legal Reference: Children's Internet Protection Act, P.L. 106-55420 U.S.C. § 6801, et seq.
47 U.S.C. § 254(h) and (l)

Procedure History:
Promulgated on: March 12, 2008
Revised: August 30, 2012
Revised: December 17, 2014