Procedure 3612-P(1): District-Provided Access to Electronic Information, Services, Equipment, and Networks - Acceptable Use of Electronic Networks

Status: ADOPTED

Original Adopted Date: 10/21/2008 **| Last Revised Date:** 09/19/2022 **| Last Reviewed Date:** 09/19/2022

District-Provided Access to Electronic Information, Services, Equipment, and Networks

All use of equipment and 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. Acceptable Use – Access to the District's equipment and electronic networks must be: (a) for the purpose of education or research and consistent with the educational objectives of the District; or (b) for legitimate business use.

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

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

   a. Using the equipment and network for any illegal activity, including violation of copyright or other contracts, or transmitting any material in violation of any federal or state law;

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

   c. Downloading copyrighted material for other than personal use;

   d. Using the equipment or network for private financial or commercial gain;

   e. Wastefully using resources, such as file space;

   f. Hacking or gaining unauthorized access to files, resources, or entities;

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

   h. Using another user's account or password;

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

   j. Posting anonymous messages;

   k. Using the equipment or network for commercial or private advertising;

   l. Accessing, submitting, posting, publishing, or displaying any defamatory, inaccurate, abusive, obscene, profane, sexually oriented, threatening, racially offensive, harassing, or illegal material; and

   m. Using the equipment or network while access privileges are suspended or revoked.

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 colleagues.

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.

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 or building principal. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's account without written permission from that individual. 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 equipment, data of another user, the Internet, or any other network. This includes but is not limited to 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 and staff engaged in producing Web pages must provide library media specialists 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.

Internet Safety

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 these procedures, and will otherwise follow these procedures.

2. Staff members shall supervise students while students are using District Internet access, 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 determined by the Superintendent or designee.

4. The district shall provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction shall include, but not be limited to: positive interactions with others online, including on social networking sites and in chat rooms; proper online social etiquette; protection from online predators and personal safety; and how to recognize and respond to cyberbullying and other threats.

5. The system administrator and principal shall monitor student Internet access.

Montana Code Annotated References	**Description**
20-5-201	Duties and Sanctions

United States Code References	**Description**
47 U.S.C. 254(h) and (l)	Universal service
P.L. 106-554	Children's Internet Protection Act,
P.L. 110-385	Broadband Data Services Improvement Act/Protecting Children in the 21st Century Act of 2008

Cross References	**Description**
2050	Innovative Student Instruction - https://simbli.eboardsolutions.com/SU/3n8jplusbrPSvskZ9ls6gSkvA==
2168	Remote Instruction from Non-District Sources - https://simbli.eboardsolutions.com/SU/jjnkfmh5AEShfiXz77kjhA==
2170	Digital Academy Classes - https://simbli.eboardsolutions.com/SU/a2toCPF6slshT9slshOplusqjoSSt5A==
2170-P(1)	Digital Academy Classes - https://simbli.eboardsolutions.com/SU/Ti55iCeUu11OHZNtHvUXLA==
3650	Montana Pupil Online Personal Information Protection Act - https://simbli.eboardsolutions.com/SU/f4plusoH59Ir0lOPhH55wqplusuw==