

Gardiner Public School

Districts 4&7

Children's Internet Protection Policy, Acceptable Use Policy and User Agreement

This document is based on Montana School Board Association Policy 3612, but has been modified to better fit with Gardiner School District needs and the expectations we have of our students.

Internet Use

Internet access is available to students and teachers in Gardiner School District. The Internet has the potential to offer vast, diverse, and unique resources to students and teachers, and to promote educational excellence through the facilitation of resource sharing, innovation, and communication.

The Internet connects myriad computers worldwide. Students and teachers have access to e-mail and chat communication with people the world over, as well as to the latest scientific information, documents and software in the public domain, university and government libraries, and wide-ranging discussion groups, to name but a few of the available resources.

With broad access to information comes the availability of material that may not be considered of value within the context of an educational setting. Gardiner School District has taken precautions to restrict access to questionable materials, with the realization that it is impossible to completely prevent an industrious user from happening upon such information by chance or design. We firmly believe that the value of the information and interaction possible on the Internet far outweighs the possibility that users may procure material that is not within the scope of the educational goals of the district.

Internet Safety

As stated above, it is nearly impossible to keep a determined student from accessing harmful or otherwise undesirable material on the Internet. That said, measures can be put in place to discourage such events from occurring. Gardiner School District uses filtering software that redirects all Internet traffic to a proxy server that blocks access to inappropriate Web sites.

The district will provide age-appropriate instruction to students regarding online behavior. This will include, but not be limited to: interacting with others online, including on social networking sites and in chat rooms; proper social etiquette when online; personal safety and protection from online predators; and how to recognize and respond to cyberbullying.

When students are allowed to use e-mail, instant messaging, or chat rooms as part of a classroom assignment, teachers are required to monitor the content of any messages sent or conversations in which students may be engaged.

No member of the Gardiner School District staff or student body is permitted to give out personal information, including photographs, about any student, minor or otherwise, via the Internet without the express **verbal and written authorization of a custodial parent or**

guardian.

Network and Internet User Agreement

Guidelines are provided here so that you are aware of the responsibilities you are about to acquire. In general, they stipulate efficient, ethical, and legal utilization of network and Internet resources. Should a Gardiner School District user violate any of these provisions, his or her account may be terminated and network, Internet, and computer access may be denied. The signature(s) at the end of this document is (are) legally binding, and indicate(s) that the part or parties who signed has (have) read the terms and conditions herein carefully, understand(s) their significance, and agree(s) to them.

Network and Internet Guidelines

1. **Acceptable use.** Internet and network use must be in support of education and research and consistent with the educational objectives of the Gardiner School District. Access and use of another entity's network must comply with the rules for use established by that entity. Transmission of any material in violation of U.S. or state regulations is prohibited. This includes but is not limited to copyrighted material, obscene or threatening material, or material protected by trade secret.
2. **Privileges.** The use of the network and the Internet is a privilege, not a right, and **inappropriate use will result in removal of the privilege.** The system administrator may close an account at any time as required, and any faculty or staff member may request that the administrator deny access to, suspend, or revoke specific user accounts.
3. **Sharing of Personal Information on the Internet.** Students are not permitted to use electronic mail and other forms of Internet communication/social networking (Facebook, Snapchat, Twitter, blogs, etc.) at school, except as part of a classroom activity that is approved and monitored by a teacher or supervisory staff member.
Devices. The use of Internet-capable personal devices (i.e., iPod Touch, smart phones, etc.) is not currently allowed except as permitted by teachers for classroom purposes, in accordance with Gardiner School District policy 3630, which governs the use of electronic signaling devices by students.
4. **Command prompt.** Students may not use the command prompt (MS-DOS prompt) for any reason, except under the supervision of the system administrator for diagnostic purposes.
5. **Downloading.** A student may not download material **of any nature**, without the express permission of, or at the request of, a teacher or administrator.
6. **Network etiquette.** Users are expected to abide by the generally accepted rules of network(Internet) etiquette, including but not limited to:
 - a. **Be polite**
 - b. **Use appropriate language**
 - c. **Maintain secrecy of personal phone numbers and addresses**
 - d. **Use discretion when giving information via the Internet (including e-mail), which may not be secure**
 - e. **Assume all information accessible over the network, including the Internet, to be the private property of the author, including e-mail**

f. The intimidation/threatening of others via the Internet (i.e., cyberbullying) is illegal, and will NOT be tolerated

- 7. Security.** Security is a high priority. If you identify a security problem on the network or Internet, notify the system administrator. Do not share the problem with other users. Do not use another individual's account. Anyone identified as a security risk, or having a history of security problems with other networks, may be denied access to the school's network. Examples of security problems include, but are not limited to, unauthorized access to the school network or any other network.
- 8. Vandalism.** Vandalism is defined as a malicious attempt to harm or destroy another user's data, to harm or destroy data on the Gardiner School or any other network, or to harm or destroy computer or network equipment.

Failure to abide by the terms above may be punished by suspension or cancellation of some or all network and computer privileges for a period of time to be determined by the school administration, or by other punishments as the school administration sees fit. Should a student's failure to abide by the terms above constitute criminal activity, the appropriate authorities will be involved.

Parent/Guardian: I have read and discussed this document with my child, and agree to its terms and conditions. I understand that my child's failure to follow the terms and conditions set forth in this document may result in disciplinary action

Parent/Guardian Signature _____ Date _____

Student: I have read and understand this document, and/or my parent/guardian has discussed it with me. I agree to follow the conditions set forth in this document.

Student Signature _____ Date _____

Modified 7/25/2016