Authorization for Electronic Network Access

General

Technology offers vast, diverse, and unique resources to both students and staff members of Colstrip Public School District #19. The district's goal in providing this service to staff and students is to promote education excellence in schools by facilitating resource sharing, innovation and communication. Technology from this point forward is meant to include the computer, phone services or any other means of network communications. User refers to any student, district employee, or community member using the network services provided by Colstrip Public School District #19.

Access to computers and people all over the world includes the availability of material that may not be considered to be of educational value in the context of the school setting. Colstrip Public School District #19 believes that the benefits of using information and interaction made available on this worldwide network far outweigh the chance that a user will procure materials not consistent with the educational goals of the district. It is the district's intent to provide guided access and supervision for students using technology.

Technology access is coordinated through a complex association of government agencies and regional and state networks. In addition, the smooth operation of the network relies upon the proper conduct of the end users who must adhere to strict policies. These procedures are provided here so the user is aware of his/her responsibilities. Users are expected to utilize technology resources in an efficient, ethical and legal manner. If a user violates any of these expectations, his/her access may be terminated, future access may be denied, and disciplinary action may be warranted.

Terms and Conditions

Acceptable Use – Access to the electronic information, services and 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.

Privileges – The use of the electronic information, services and networks is a privilege, not a right, and inappropriate use will result in cancellation of those privileges. The system administrator (and/or building 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.

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, 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 without virus;

c. Downloading copyrighted material for other than personal use;

d. Using the 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 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 network while access privileges are suspended or revoked.

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.

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.

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.

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.

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, or any other network. This includes but is not limited to uploading or creation of computer viruses.

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.

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.

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 and staff members in fulfilling their duties and responsibilities and as an education tool.

b. 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 or staff member to an electronic mail account is strictly prohibited.

c. 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.

d. 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.

e. Any message received from an unknown sender via the Internet should either be immediately deleted or forwarded to the system administrator. 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.

f. Use of the District's electronic mail system constitutes consent to these regulations.

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 building principals shall monitor student Internet access.

On-line Education Component:

Before authorization for network access can be granted, all users must successfully complete the Colstrip Public Schools #19 Internet Safety and Digital Citizenship curriculum basics.

a. Cyberbullying
b. Privacy and Information Sharing
c. Social Networking Safety
d. Online Predator Safety

This agreement is for the sole purpose of clarification in accordance with Board Policy *3612 District Provided Access to Electronic Information, Services and Networks, 3620 Bring Your Own Device (BYOD).* Violation of any policy or procedure is subject to disciplinary actions specified in the handbook. The system administrator reserves the right to terminate/restrict a user's privileges as needed.

The District will only create network account(s) for minors if the Guardian signs the Consent Form. All network users are accepting the terms of all policies and procedures of Colstrip Pubic Schools #19 by logging into the District's electronic network.

This *Authorization for Electronic Network Access* administrative procedure may be revised at any time by the District without prior notice. Please refer to the most current version of this procedure as posted on the District's website.

Electronic Use Agreement

Student:

I have read the *Authorization for Electronic Network Access* and viewed the *Internet Safety Basics* component of the *Internet Safety and Digital Citizenship* curriculum. I understand that Internet sites are filtered and that use on a district computer or device and the district network may be monitored. I hereby agree to comply with the described conditions of acceptable use.

Student Signature_____Date_____

Student name (please print)_____

Parent or Guardian:

As the parent or guardian of the above named student, I have read the *Authorization for Electronic Network Access* and understand that Internet sites are filtered and that electronic information resource accounts may be monitored. I understand my child may be disciplined for inappropriate or unacceptable use of electronic information resources. I further understand that student use of the electronic information resource system is designed for educational purposes. I understand that it is impossible for the district to filter or restrict access to all inappropriate materials. I will not hold the District responsible for inappropriate or unacceptable materials my child may acquire on the network system.

I hereby give my permission and approve the issuance of an electronic account for my child.

Parent or Guardian Signature_____

Parent or Guardian Name (printed)_____ Date _____

Student Name_____