Great Falls School District

STUDENTS 3612P

Student Computer Acceptable Use and Internet Safety Agreement

Great Falls Public Schools is pleased to offer our student's access to equipment, the Internet and other electronic networks. The advantages afforded by the rich, digital resources available today outweigh any disadvantage. However, it is important to remember that access is a privilege, not a right, and carries with it responsibilities of digital citizenship for all involved.

Terms of Agreement

PLEASE REVIEW THE AGREEMENT BELOW AND CHECK THE APPROPRIATE BOX ON THE STUDENT/PARENT SIGN-OFF PAGE OF THE STUDENT HANDBOOK.

In order for a student to be allowed access to a school district electronic device, network, and the Internet, parents and students must review the agreement below, check the appropriate box on the student/parent sign-off page of the student handbook, sign and return annually.

Student Acceptable Uses

The District provides equipment, electronic information, services, and networks for all educational purposes. All use must be in support of education and/or research, and in furtherance of the District's stated educational goals. Accordingly, regulations for participation by anyone on the Internet shall include but may not be limited to the following:

- Access is a privilege, not a right, and carries with it responsibilities of digital citizenship for all involved. Students will use appropriate language and/or images (e.g. no swearing, vulgarities, suggestive, obscene, inflammatory, belligerent, or threatening language and/or images). Students will practice respect for others, by never using any technology to harass, haze, intimidate or bully anyone.
- Students are responsible for all activity under their electronic accounts. Students will not share passwords with other users or log in as someone other than themselves. The only exception may be teachers safeguarding the passwords of his/her students. Students will log off of devices and/or websites when finished.
- Students will use school district-provided devices, networks, and Internet access for educational purposes only. Uses that promote a personal commercial enterprise for personal gain through selling or buying over the school district's network are prohibited. Uses in regards to political agendas must be in compliance with state law and Board policy.
- Students will protect their privacy of self and others. Students will carefully safeguard last names, personal addresses, personal phone numbers, personal email addresses, password, photos, or other personal information on the Internet, including such items

belonging to others. Students should be aware that when using many digital tools on the Internet, published work may be publicly accessible and permanently available.

- The District reserves the right to monitor, inspect, backup, and review and store at any time and without prior notice, any and all usage of the school district equipment, network and Internet access, and any and all information transmitted or received in connection with such usage. This also includes any information stored on school district network or local electronic devices. All such information files shall be and remain accessible by the District, and no students shall have any expectation of privacy regarding such information. Students are advised that all material in whatever form in the school district system's network may be considered public record pursuant to MCA 2-6-102.
- Student Photos/Student Work. Publishing student pictures and work on websites promotes learning, collaboration, and provides an opportunity to share the achievements of students. If parents/guardians do not want release or student directory information, including photos and school work, school must be notified in writing (see page 2 of the District's Student Handbook).
- While the District makes every effort to filter inappropriate material, it is possible for an industrious user to gain access to such material. Inappropriate material is defined as material that violates generally accepted social standards. It is the student's responsibility not to initiate access to or to distribute inappropriate material or attempt to circumvent filters.
- It is every student's responsibility to adhere to the copyright laws of the United States (P.L. 94-553) and the Congressional Guidelines that delineate those laws regarding software, authorship, and copying information.
- It is every student's responsibility to treat the physical and digital property of others with respect. This includes proper treatment of digital services and other hardware, the network system, and respecting other's electronic files. Students are not to remove, and/or modify software, computer hardware or network equipment without prior Information Technology Department authorization.

<u>Student Responsibilities</u>

Students understand that access is a privilege, not a right, and carries with it responsibilities of digital citizenship for all involved. Students understand that if they choose not to follow the rules, they may lose computer privileges and/or have other consequences.

Limitations of Use. Students must refrain from these activities, none of which are all inclusive:

- Uses that violate local, state and/or federal laws or encourage others to violate the law.
- Uses that include the transmission of offensive or harassing messages.
- Uses that offer for sale or use any substance of which the possession or use of is prohibited by the District's student discipline policy.
- Uses that violate generally accepted social standards of public communication such as the access of:
    - Pornographic, sexual, or obscene content;
    - Personal dating or connection sites;
    - Drugs, alcohol and gambling content: and/or

    - Hate speech, violence, weapons and cult content.
- Uses that intrude into the equipment, networks or information owned by others.
- Uses that include the downloading or transmitting of confidential, trade secret, or copyrighted information or materials.
- Uses that cause harm to others or damage to their property.
- Uses that engage in defamation (harming another's reputation by lies).
- Uses that employ another's password.
- Uses that mislead message recipients into believing that someone other than the sender is communicating, or otherwise using his/her access to equipment, the network or the Internet.
- Uses that cause the uploading of a worm, virus, or other harmful forms of programming or vandalism.
- Uses that are "hacking" or any form of unauthorized access to other equipment, networks, or other information.
- Uses that jeopardize the security of student access and of the equipment, computer network or other networks on the Internet.
- Uses that promote a personal commercial enterprises for personal gain through selling or buying over the District's network.
- Uses that promote an individual's political agenda to include soliciting support for or opposition to any political committee, the nomination or election of any person to public office, or the passage of a ballot issue.
- Uses of posting anonymous messages.
- Uses of the equipment, network or Internet while access privileges are suspended or revoked.

Password Protection. Users' network passwords are provided for their personal use, therefore, students are expected to protect their own and other's passwords. In order to do so, note the following:

- Students should not share their password with anyone.
- Students should not log into the network with another user's login name and password.
- If a student suspects someone has discovered their password, they should change it or have it changed immediately.
- Students shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.
- Student should log off District devices when finished.

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 equipment, data of another user, the Internet, or any other network. This includes but is not limited to uploading or creation of computer viruses.

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.

- 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.
- Students and staff engaged in producing Web pages must provide library media specialist with email or hard copy permissions before the Web pages are published. Printed evidence of the status of "public domain" documents must be provided.
- 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.
- The "fair use" rules governing student reports in classrooms are less stringent and permit limited use of graphics and text.
- Student work may only be published if there is written permission from both the parent/guardian and the student.

Other Expectations.

- Students must print only with permission from a teacher.
- Students must tell a teacher if he/she reads or sees something on a device that is inappropriate and/or limited (See above list of limitations.)
- Students must tell a teacher if a device has been changed in any way.

<u>Teacher Responsibilities</u>

Teachers will provide guidance to students as they access equipment, electronic information, services and networks for educational purposes. Teachers will:

- Inform all students of their rights and responsibilities as users of the district network prior to granting access to that network, either as an individual user or as a member of a class or group.
- Monitor when students are accessing the Internet.
- Address student infractions of the Acceptable Use Agreement according to the school discipline policy.
- Provide curriculum-appropriate alternate activities for students who do not have permission to use the Internet or a particular digital tool.
- Guide student use of identifiable photographs, referencing student directory release of information.
- Follow the Children's Online Protection Act (COPPA) guidelines when using digital tools in the classroom.
- Provide age-appropriate instruction to students regarding appropriate online behavior. Such instruction shall include, but not 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.
- Submit a Request for Software/App Review form when seeking to use new software or apps. Approval from the Director of Information Technology must be received before using. If needed, a Data Privacy Agreement must be completed and signed by authorized Great Falls Public Schools personnel and the software vendor as required by MCA 20-7-1323-1326.

<u>Principal Responsibilities</u>

Principals will provide support to teachers and students in following the Student Computer Acceptable Use and Internet Safety Agreement. Principal shall:

- Address student infractions of the Acceptable Use Agreement according to the school discipline policy.
- Provide an updated list of students who do not have permission to use the Internet, to use particular digital tools, to take technology home, or to have works or images displayed online.

<u>District Responsibilities</u>

The District will provide support to principals, teachers, and students in following the Student Computer Acceptable Use and Internet Safety Agreement. The District will:

- Ensure that Children's Internet Protection Act (CIPA) compliant filtering technology is in use.
- Review the Staff and Student Acceptable Use Agreement as necessary. Staff annually reviews this policy.
- Provide professional development for staff regarding expected behavior concerning this agreement.
- Ensure curriculum reflects digital citizenship

- Monitors Internet activity and provides Internet usage reports to principals for possible disciplinary action.
- Reviews new requests for software/apps and ensures Data Privacy Agreements are completed as required by MCA 20-7-1323-1326.

Acceptable Uses of Personal Devices on the District Network

Students may bring their own personal electronic devices which may or may not be able to connect to the District/school wireless network. When using personal electronic devices, students must abide by the Acceptable Use Agreement, in addition to the following. Students will:

- Use personal devices in class only with the teacher's express permission.
- Only connect to the District/school wireless guest network and NOT to the District/school wired network. Students understand if their personal device is found wired to the District/school network, the device will be removed and turned into the administrator.
- Only use devices with up-to-date virus protection software.
- Turn off all peer-to-peer (music/video/file-sharing) software or web-hosting services on their device while connected to the District/school wireless network.
- Understand the security, care, and maintenance of their device is their responsibility. Student devices will be securely stored when not in use.
- Understand that the District/school is not responsible for the loss, theft, or damage of student devices. Students are fully responsible for their property while at school. Students understand that if they should leave their device in the custody of a staff member, that the staff member is not responsible for the loss, theft, or damage of the student device.
- Understand the Information Technology Department will not provide support for personal devices. Students are fully responsible for making their device work within the parameters defined in this agreement. If they are unable to make their personal device work within these parameters and the given time allotted by the teacher, the student will need to use a device that is provided by the District/school to prevent any interruption to instruction and learning.
- Understand that school staff may access student personal electronic devices if there is reasonable suspicion that the search will uncover evidence that they are violating the law, Board policy, administrative regulation, or other rules of the District/ ~~of the~~ school. This may include, but is not limited to, audio and video recording, photographs taken on District/school property that violates the privacy of others, issues regarding bullying, verification that the student's device is connected to the District/school network, etc. Students will provide appropriate login credentials to the device if required. Failure to provide access is insubordination and will be deemed satisfactory evidence that the student device contains content that violates this section.
- Not use audio/video recording device, to record media or take photos during school hours unless given permission from both a staff member and those being recorded.

Failure to Follow Acceptable Use Agreement

Use of the school district electronic equipment, network, and Internet is a privilege, not a right. A student who violates this agreement is subject to disciplinary action according to District Policy. Note that some infractions of the Acceptable Use Agreement may be criminal, and as such, legal action may be taken.

References:

Policy 3225	Sexual Harassment/Intimidation of Students
Policy 3226	Hazing, Harassment, Intimidation, Bullying
Policy 3231	Searches and Seizure
Policy 3300	Corrective Actions and Punishments
Policy 3310	Student Discipline
Policy 3630	Cellular Telephone and Electronic Signaling Device Policy
Policy 3612	District-Provided Access to Electronic Information, Equipment, Services, and Network
Policy 5450	Employee Electronic Mail and Online Services Usage
Policy 5450F	Staff Computer Acceptable Use and Internet Safety Agreement
Policy 5460	Electronic Resources and Social Networking

Legal References:

Family Education Rights and Privacy Act (FERPA)
Children's Online Privacy and Protection Act (COPPA)
Children's Internet Protect Act (CIPA)
MCA 20-7-1323-1326 Montana Pupil Online Personal Information Protection Act

Policy History

Adopted on: July 9, 2018
Revised on: August 22, 2022