

1 Great Falls School District

2  
3 **STUDENTS**

3612P

4  
5 Student Technology Acceptable Use and Internet Safety Agreement

6  
7 Great Falls Public Schools is pleased to offer our students access to District equipment,  
8 electronic networks, and Internet access. The advantages afforded by the rich, digital resources  
9 available today outweigh any disadvantage. However, it is important to remember that access is a  
10 privilege, not a right, and carries with it responsibilities of digital citizenship for all involved.

11  
12 Terms of Agreement

13  
14 **PLEASE REVIEW THE AGREEMENT BELOW AND ELECTRONICALLY INDICATE**  
15 **YOUR ACCEPTANCE OF THIS AGREEMENT BY CHECKING THE BOX “I have**  
16 **received, reviewed, and agree to the information contained in the Great Falls Public**  
17 **Schools Student Technology Acceptable Use and Internet Safety Agreement.”**

18  
19 In order for a student to be allowed access to a District-provided electronic device, electronic  
20 networks, and Internet access, parents and students must review the agreement below, and  
21 electronically accept by checking the box in PowerSchool, “I have received, reviewed, and agree  
22 to the information contained in the Great Falls Public Schools Student Technology Acceptable  
23 Use and Internet Safety Agreement.”

24  
25 Student Acceptable Uses

26  
27 The District provides equipment, electronic information, services, and networks for all  
28 educational purposes. All use must be in support of education and/or research, and in furtherance  
29 of the District’s stated educational goals. Accordingly, regulations for participation by anyone on  
30 the Internet shall include but may not be limited to the following:

- 31
- 32 • Access is a privilege, not a right, and carries with it responsibilities of digital citizenship  
33 for all involved. Students will use appropriate language and/or images (e.g. no swearing,  
34 vulgarities, suggestive, obscene, inflammatory, belligerent, or threatening language  
35 and/or images). Students will practice respect for others, by never using any technology  
36 to harass, haze, intimidate or bully anyone.
  - 37 • Students are responsible for all activity under their electronic accounts. Students will not  
38 share passwords with other users or log in as someone other than themselves. The only  
39 exception may be teachers safeguarding the passwords of their students. Students will log  
40 off of devices and/or websites when finished.
  - 41 • Students will use District-provided devices, electronic networks, and Internet access for  
42 educational purposes only. Uses that promote a personal commercial enterprise for  
43 personal gain through selling or buying over the District-provided network are prohibited.  
44 Uses in regard to political agendas must be in compliance with state law and Board  
45 policy.

- 1 • Students will protect the privacy of self and others. Students will carefully safeguard last  
2 names, personal addresses, personal phone numbers, personal email addresses, password,  
3 photos, or other personal information on the Internet, including such items belonging to  
4 others. Students should be aware that when using many digital tools on the Internet,  
5 published work may be publicly accessible and permanently available.
- 6 • The District reserves the right to monitor, inspect, backup, review, and store at any time  
7 and without prior notice, any and all usage of the District-provided equipment, electronic  
8 networks and Internet access, and any and all information transmitted or received in  
9 connection with such usage. This also includes any information stored on District  
10 network or local electronic devices. All such information files shall be and remain  
11 accessible by the District, and no students shall have any expectation of privacy regarding  
12 such information. Students are advised that all material in whatever form on the District  
13 network may be considered public record pursuant to MCA 2-6-102.
- 14 • Publishing student pictures and work on websites promotes learning, collaboration, and  
15 provides an opportunity to share the achievements of students. If parents/guardians do not  
16 want the release of student directory information, including photos and school work, they  
17 must electronically check the corresponding boxes in the Release of Student Information  
18 section in PowerSchool.
- 19 • While the District makes every effort to filter inappropriate material, it is possible for a  
20 persistent user to gain access to such material. Inappropriate material is defined as  
21 material that violates generally accepted social standards. It is the student's responsibility  
22 not to initiate access to or to distribute inappropriate material or attempt to circumvent  
23 District security measures.
- 24 • It is every student's responsibility to adhere to the copyright laws of the United States  
25 (P.L. 94-553), the Congressional Guidelines that delineate those laws regarding software,  
26 authorship, and copying information, and the academic honesty requirements of Board  
27 policy.
- 28 • It is every student's responsibility to treat the physical and digital property of others with  
29 respect. This includes proper treatment of digital services and other hardware, the  
30 network system, and respecting other's electronic files. Students are not to remove,  
31 and/or modify software, computer hardware or network equipment without prior  
32 Information Technology Department authorization.

### 33 Student Responsibilities

34 Students understand that access is a privilege, not a right, and carries with it responsibilities of  
35 digital citizenship for all involved. Students understand that if they choose not to follow the  
36 rules, they may lose technology access privileges and/or have other consequences.  
37

38 **Limitations of Use.** Students must refrain from these activities, none of which are all inclusive:  
39

- 40 • Uses that violate local, state and/or federal laws or encourage others to violate the law.
- 41 • Uses that include the transmission of offensive or harassing messages.
- 42 • Uses that offer for sale or promote the use of any substance of which the possession or  
43 use of is prohibited by the District's student discipline policy.
- 44
- 45

- 1 • Uses that violate generally accepted social standards of public communication such as the  
2 access of:
  - 3 ○ Pornographic, sexual, or obscene content;
  - 4 ○ Personal dating or connection sites;
  - 5 ○ Drugs, alcohol and gambling content: and/or
  - 6 ○ Hate speech, violence, weapons and cult content.
- 7 • Uses that intrude into the equipment, networks or information owned by others.
- 8 • Uses that include the downloading or transmitting of confidential, trade secret, or  
9 copyrighted information or materials.
- 10 • Uses that cause harm to others or damage to their property.
- 11 • Uses that engage in defamation (harming another's reputation by lies).
- 12 • Uses that employ another's password.
- 13 • Uses that mislead message recipients into believing that someone other than the sender is  
14 communicating, or otherwise using their access to District-provided equipment,  
15 electronic networks, or Internet access.
- 16 • Uses that cause the uploading of a worm, virus, or other harmful forms of programming  
17 or vandalism.
- 18 • Uses that are "hacking" or any form of unauthorized access to other equipment,  
19 networks, or other information.
- 20 • Uses that jeopardize the security of student access and of the equipment, computer  
21 network or other networks on the Internet.
- 22 • Uses that promote a personal commercial enterprise for personal gain through selling or  
23 buying over the District's network.
- 24 • Uses that promote an individual's political agenda to include soliciting support for or  
25 opposition to any political committee, the nomination or election of any person to public  
26 office, or the passage of a ballot issue.
- 27 • Uses that contain anonymous messages.
- 28 • Uses of equipment, electronic networks, or Internet access while access privileges are  
29 suspended or revoked.

30  
31 **Password Protection.** Users' network passwords are provided for their personal use; therefore,  
32 students are expected to protect their own and other's passwords. In order to do so, note the  
33 following:

- 34
- 35 • Students should not share their password with anyone; age and ability appropriate  
36 exceptions are made for students who may need to rely on staff for password  
37 management.
- 38 • Students should not log into the network using any username and password other than  
39 their own.
- 40 • If a student suspects someone has discovered their password, they should change it or  
41 have it changed immediately.
- 42 • Students shall not intentionally seek information on, obtain copies of, or modify files,  
43 other data, or passwords belonging to other users.
- 44 • Students should log off District-provided equipment and electronic networks when  
45 finished.

- Students must change passwords when directed by the District.

**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 creating computer viruses.

**Copyright Rules for Internet Publication.** Copyright law and District policy prohibit the republishing of text or graphics found on the Internet 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 follow the established District guidelines for Internet publication. Evidence of the status of "public domain" documents must be posted.
- 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 as indicated electronically in the Release of Student Information.

**Other Expectations.**

- 1 • Students must print only with permission from a teacher.
- 2 • Students must tell a teacher if they read or see something on a device that is inappropriate
- 3 and/or limited (see above list of limitations.)
- 4 • Students must tell a teacher if a device has been changed in any way.

### 6 Teacher Responsibilities

7  
8 Teachers will provide guidance to students as they access District-provided equipment,  
9 electronic networks, and Internet access for educational purposes. Teachers will:

- 10 • Inform all students of their rights and responsibilities as users of District-provided
- 11 equipment, electronic networks, and Internet access prior to granting access to those
- 12 resources, either as an individual user or as a member of a class or group.
- 13 • Monitor when students are accessing the Internet.
- 14 • Address student infractions of the Acceptable Use Agreement according to the school
- 15 discipline policy.
- 16 • Provide curriculum-appropriate alternate activities for students who do not have
- 17 permission to use the Internet or a particular digital tool.
- 18 • Guide student use of identifiable photographs, referencing student directory release of
- 19 information.
- 20 • Follow the Children’s Online Privacy Protection Act (COPPA) guidelines when using
- 21 digital tools in the classroom.
- 22 • Provide age-appropriate instruction to students regarding appropriate online behavior.
- 23 Such instruction shall include, but not be limited to: positive interactions with others
- 24 online, including on social networking sites, and in chat rooms; proper online social
- 25 etiquette; protection from online predators and personal safety; and how to recognize and
- 26 respond to cyberbullying and other threats.
- 27 • Submit a Request for Software/App Review form when seeking to use new software or
- 28 apps. Approval from the Director of Information Technology must be received before
- 29 using. If needed, a Data Privacy Agreement must be completed and signed by authorized
- 30 Great Falls Public Schools personnel and the software vendor as required by MCA 20-7-
- 31 1323-1326.

### 32 33 Principal Responsibilities

34  
35 The Principal or designee will provide support to teachers and students in following the Student  
36 Technology Acceptable Use and Internet Safety Agreement. The Principal or designee shall:

- 37  
38 • Address student infractions of the Acceptable Use Agreement according to the school
- 39 discipline policy.
- 40 • Maintain an updated list of students who do not have permission to use the Internet, to
- 41 use particular digital tools, to take technology home, or to have works or images
- 42 displayed online.
- 43 • Notify the Informational Technology (IT) department whenever changes occur.

### 44 45 District Responsibilities

46

1 The District will provide support to staff and students in following the Student Technology  
2 Acceptable Use and Internet Safety Agreement. The District will:

- 3
- 4 • Ensure that Children’s Internet Protection Act (CIPA) compliant filtering technology is in
- 5 use.
- 6 • Review the Staff and Student Acceptable Use Agreement as necessary. Staff annually
- 7 review this policy.
- 8 • Provide professional development for staff regarding expected behavior concerning this
- 9 agreement.
- 10 • Ensure curriculum reflects digital citizenship
- 11 • Monitors Internet activity and provides Internet usage reports to principals for possible
- 12 disciplinary action.
- 13 • Reviews new requests for software/apps and ensures Data Privacy Agreements are
- 14 completed as required by MCA 20-7-1323-1326.
- 15

### 16 Acceptable Uses of Personal Devices on the District Network

17

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

- 21
- 22 • Use personal devices in class only with the teacher’s express permission.
- 23 • Only connect to the District/school wireless guest network and NOT to the
- 24 District/school wired network. Students understand if their personal device is found wired
- 25 to the District/school network, the device will be removed and turned into the
- 26 administrator.
- 27 • Only use devices with up-to-date virus protection software.
- 28 • Turn off all peer-to-peer (music/video/file-sharing) software or web-hosting services on
- 29 their device while connected to the District/school wireless network.
- 30 • Understand the security, care, and maintenance of their device is their responsibility.
- 31 Student devices will be securely stored when not in use.
- 32 • Understand that the District/school is not responsible for the loss, theft, or damage of
- 33 student devices. Students are fully responsible for their property while at school. Students
- 34 understand that if they should leave their device in the custody of a staff member, the
- 35 staff member is not responsible for the loss, theft, or damage of the student device.
- 36 • Understand the Information Technology Department will not provide support for
- 37 personal devices. Students are fully responsible for making their device work within the
- 38 parameters defined in this agreement. If they are unable to make their personal device
- 39 work within these parameters and the given time allotted by the teacher, the student will
- 40 need to use a device that is provided by the District/school to prevent any interruption to
- 41 instruction and learning.
- 42 • Understand that school staff may access student personal electronic devices if there is
- 43 reasonable suspicion that the search will uncover evidence that they are violating the law,
- 44 Board policy, administrative regulation, or other rules of the District/school. This may
- 45 include, but is not limited to, audio and video recording, photographs taken on
- 46 District/school property that violates the privacy of others, issues regarding bullying,

1 verification that the student’s device is connected to the District/school network, etc.  
2 Students will provide appropriate login credentials to the device if required. Failure to  
3 provide access is insubordination and will be deemed satisfactory evidence that the  
4 student device contains content that violates this section.

- 5 • Not use audio/video recording devices, to record media or take photos during school  
6 hours unless given permission from both a staff member and those being recorded.

7  
8 Failure to Follow Acceptable Use Agreement

9  
10 Use of the District-provided equipment, electronic networks, and Internet access is a privilege,  
11 not a right. A student who violates this agreement is subject to disciplinary action according to  
12 District Policy. Note that some infractions of the Acceptable Use Agreement may be criminal,  
13 and as such, legal action may be taken.  
14

15 References:

16 Policy 3225	Sexual Harassment/Intimidation of Students
17 Policy 3226	Hazing, Harassment, Intimidation, Bullying
18 Policy 3231	Searches and Seizure
19 Policy 3300	Corrective Actions and Punishments
20 Policy 3310	Student Discipline
21 Policy 3310P2	Academic Honesty and Responsible Use of Resources
22 Policy 3630	Cellular Telephone and Electronic Signaling Device Policy
23 Policy 3612	District-Provided Access to Electronic Information, Equipment, 24 Services, and Network
25 Policy 5450	Employee Electronic Mail and Online Services Usage
26 Policy 5450F	Staff Computer Acceptable Use and Internet Safety Agreement
27 Policy 5460	Electronic Resources and Social Networking

28  
29 Legal References:

30 Family Education Rights and Privacy Act (FERPA)	
31 Children’s Online Privacy and Protection Act (COPPA)	
32 Children’s Internet Protect Act (CIPA)	
33 § 20-7-1323-1326, MCA	Montana Pupil Online Personal Information Protection Act

34  
35  
36 Policy History

37 Adopted on:	July 9, 2018
38 Revised on:	August 22, 2022
39 Revised on:	May 11, 2026