

1 Great Falls School District

2  
3 **PERSONNEL**

5450F

4  
5 Staff Technology Acceptable Use and Internet Safety Agreement

6  
7 Great Falls Public Schools offers our staff access to District-provided equipment, electronic  
8 networks, and Internet access. It is important to remember that access is a privilege, not a right,  
9 and carries with it responsibilities of digital citizenship for all involved. Inappropriate use will  
10 result in cancellation of those privileges. The Superintendent or designee will make all decisions  
11 regarding whether or not a user has violated these procedures and may monitor, deny, revoke, or  
12 suspend access at any time.

13  
14 Terms of Agreement

15  
16 In order for a staff member to obtain access to District-provided equipment, electronic  
17 networks, and Internet access, the staff member must sign an Acceptable Use Form at the time  
18 of employment. The signed consent form is kept in their employee file.

19  
20 Staff Acceptable Uses

21  
22 The District provides electronic information, services, and networks for educational purposes.  
23 All use must be in support of education and/or research, and in furtherance of the District's  
24 stated educational goals. Accordingly, regulations for participation by staff on the Internet shall  
25 include but may not be limited to the following:

- 26
- 27 • Use of electronic e-mail, computer networks and online telecommunications is a  
28 privilege and must support teaching, learning, research, the employee's work and the  
29 school environment.
  - 30 • Use for informal or personal purposes is permissible within reasonable limits.
  - 31 • Students, parents, faculty, and staff in Great Falls Public Schools will have access to  
32 web-based educational resources in compliance with local, state, and federal laws.
  - 33 • Authorized users will be ultimately responsible for all activity under their account and  
34 password. Accounts will be used only by the authorized user for the purposes specified.  
35 Unauthorized use of an identity or password other than the user's own is prohibited  
36 Allowing students or coworkers permission to use your password is a direct violation of  
37 this policy. All network users will adhere to the rules of copyright regarding software,  
38 information, and the attribution of authorship. Reposting communications without the  
39 author's permission or without proper attribution is prohibited.
  - 40 • Any use of telecommunication services or networks for illegal, inappropriate, obscene,  
41 or pornographic purposes are prohibited. Illegal activities are defined as a violation of  
42 local, state, and/or federal laws. Inappropriate use is defined as a violation of the  
43 intended use of the District's mission, goals, policies, or procedures. Obscenity and/or  
44 pornography is defined as a violation of generally accepted social standards for use of a  
45 publicly owned and operated communication vehicle. Any user who accesses obscenity  
46 and/or pornography will face disciplinary action that may result in immediate

1 termination. Users will report to immediate supervisor, any inadvertently accessed  
2 unsuitable material immediately.

- 3 • All use of telecommunication services or networks for the promotion of an individual's  
4 personal or political agenda or commercial initiatives are prohibited.
- 5 • Use of or engaging in offensive or inflammatory speech, profanity, or obscene language  
6 is not permitted at any time.
- 7 • Hate mail, harassment, discriminatory remarks, and other antisocial behaviors are not  
8 permitted.
- 9 • Users will not intentionally download unauthorized software, spread computer viruses,  
10 vandalize the data, infiltrate systems, damage hardware or software, or in any way  
11 degrade or disrupt the use of the network. If staff believe their computer is  
12 compromised, they should report it to the IT Help Desk immediately. Hacking or  
13 gaining unauthorized access to files, resources, or entities is prohibited.
- 14 • Individuals will follow confidentiality procedures when accessing personal information  
15 about students or employees and only release confidential information with proper  
16 authorization and consent per Family Educational Rights and Privacy Act ([FERPA](#))  
17 regulations. Invading the privacy of individuals, which includes the unauthorized  
18 disclosure, dissemination, and use of information of a personal nature about anyone is  
19 prohibited.
- 20 • Users will maintain professional standards of behavior as detailed in the Professional  
21 Educators of Montana Code of Ethics and Board Policy 5460 which details the use of  
22 social networking.
- 23 • The District reserves the right to monitor, inspect, backup, review, and store, at any time  
24 and without prior notice, any and all usage of the District-provided equipment, electronic  
25 networks, Internet access, and all information transmitted or received in connection with  
26 such usage. This also includes any information stored on the District-provided network  
27 or local electronic devices. All such information will be and remain accessible by the  
28 District, and no staff will have any expectation of privacy regarding such information.  
29 Staff are advised that all material in whatever form ~~is~~ on the ~~school~~ District-provided  
30 network may be considered public record pursuant to MCA 2-6-102.
- 31 • Publishing student pictures and work on websites can promote learning and  
32 collaboration, and provide an opportunity to share the achievements of students. If  
33 parents/guardians do not want the release of student directory information, including  
34 photos and school work, they must electronically check the corresponding boxes in the  
35 Release of Student Information section in PowerSchool. Staff are responsible for  
36 checking student files for parental directives before posting student work online.
- 37 • It is the responsibility of each staff member to treat the physical and digital property of  
38 others with respect. This includes proper treatment of District-provided equipment,  
39 electronic networks, and others' electronic files. Staff are not to remove, add or modify  
40 software, computer hardware or network equipment without prior Informational  
41 Technology Department authorization.
- 42 • Uses that promote an individual's political agenda, to include soliciting support for or  
43 opposition to any political committee, the nomination or election of any person to public  
44 office, or the passage of a ballot issue, are not permitted per Board Policy 5224 Political  
45 Activity – Staff Participation.
- 46 • Posting anonymous messages is not permitted.

- 1 • Staff will not use the network while access privileges are suspended or revoked.
- 2 • Passwords will be changed annually as prompted by the system.

3  
4 **Staff Responsibilities for Student Compliance.** Staff are responsible for ensuring student  
5 compliance with the District’s guidelines and expectations as listed below. Therefore, staff are  
6 responsible for understanding these guidelines and expectations.

7  
8 All student use must be in support of education and/or research, and in furtherance of the  
9 District’s stated educational goals. Accordingly, the following limitations, protections and  
10 expectations must be followed for students to have the privilege of digital access.

11  
12 **Limitations of Use.** Individuals must refrain from these activities, none of which are all  
13 inclusive:

- 14 • Uses that violate local, state, and/or federal laws or encourage others to violate the law.
- 15 • Uses that include the transmission of offensive or harassing messages.
- 16 • Uses that offer for sale or promotes the use of any substance of which the possession or
- 17 use of is prohibited by the District’s student discipline policy.
- 18 • Uses that violate generally accepted social standards of public communication such as
- 19 the access of:
  - 20 ○ Pornographic, sexual, or obscene content;
  - 21 ○ Personal dating or connection sites;
  - 22 ○ Drugs, alcohol, and gambling content; and/or
  - 23 ○ Hate speech, violence, weapons, and cult content.
- 24 • Uses that intrude into the networks, computers or information owned by others.
- 25 • Uses that include the downloading or transmitting of confidential, trade secret, or
- 26 copyrighted information or materials.
- 27 • Uses that cause harm to others or damage to their property.
- 28 • Uses that engage in defamation (harming another’s reputation by spreading false
- 29 information).
- 30 • Uses that employ another’s password.
- 31 • Uses that mislead message recipients into believing that someone other than the sender
- 32 is communicating, or otherwise using their access to the network or the Internet.
- 33 • Uses that cause the uploading of a worm, virus, other harmful form of programming, or
- 34 vandalism.
- 35 • Uses that are “hacking” or any form of unauthorized access to other computers,
- 36 networks, or other information.
- 37 • Uses that jeopardize the security of student access and of the District-provided
- 38 equipment, electronic networks, or Internet access.
- 39 • Uses that promote a personal commercial enterprise for personal gain through selling or
- 40 buying over the District’s network.
- 41 • Uses that promote an individual’s political agenda to include soliciting support for or
- 42 opposition to any political committee, the nomination or election of any person to public
- 43 office, or the passage of a ballot issue.
- 44 • Uses that contain anonymous messages.
- 45

- Uses of the equipment, network or Internet while access privileges are suspended or revoked.

**Password Protections.** 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:

- Individuals should not share their password with anyone; age and ability appropriate exceptions are made for students who may need to rely on staff for password management.
- Individuals should not log into the network using another user's login username and password other than their own.
- If an individual suspects someone has discovered their password, they should change it or have it changed immediately.
- Individuals shall not intentionally seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users.
- Individuals should log off District-provided equipment and electronic networks when finished.
- Individuals 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 Director of Information Technology or designee. Do not demonstrate the problem to other users. Keep your account and password confidential. Do not use another individual's username and password to gain access to District-provided equipment or electronic networks. 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 and Damage.** 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. The user is responsible for any unintentional damage to District-owned equipment or technology that is caused by the use or user's negligence, including but not limited to drops, spills, virus, exposure to heat and cold, or submersion.

1  
2 **Copyright Rules of Internet Publishing.** Copyright law and District policy prohibit the  
3 republishing of text or graphics found on the Internet or on District websites of file servers,  
4 without explicit written permission.

- 5  
6
- 7 • For each republication (on a website or file server) of a graphic or text file that was  
8 produced externally, there must be a notice at the bottom of the page crediting the  
9 original producer and noting how and when permission was granted. If possible, the  
10 notice should also include the web address of the original source.
  - 11 • Individuals and staff engaged in producing webpages must follow the established  
12 District guidelines for Internet publication. Evidence of the status of “public domain”  
13 documents must be posted.
  - 14 • The absence of a copyright notice may not be interpreted as permission to copy the  
15 materials. Only the copyright owner may provide the permission. The manager of the  
16 website displaying the material may not be considered a source of permission.
  - 17 • The “fair use” rules governing student reports in classrooms are less stringent and permit  
18 limited use of graphics and text.
  - 19 • Student work may only be published as indicated electronically in the Release of Student  
20 Information.

### 21 **Other Expectations**

- 22
- 23 • Students must print only with permission from a teacher.
  - 24 • Students must tell a teacher if they read or see something on a device that is  
25 inappropriate and/or limited (See above list of limitations).
  - 26 • Students must tell a teacher if a device has been changed in any way.
  - 27 • Students should be polite and use appropriate language.

### 28 Staff Responsibilities

29  
30  
31 Staff will provide guidance to students as they access District-provided equipment, electronic  
32 networks, and the Internet for educational purposes. Staff will:

- 33
- 34 • Inform all students of their rights and responsibilities as users of the District-provided  
35 equipment electronic networks, and Internet access prior to granting access to those  
36 resources, either as an individual user or as a member of a class or group.
  - 37 • Monitor students when they are accessing the Internet.
  - 38 • Address student infractions of the Student Technology Acceptable Use and Internet  
39 Safety Agreement according to the school discipline policy.
  - 40 • Work with administration to provide curriculum-appropriate alternative activities for  
41 students who do not have permission to use the Internet or a particular digital tool.
  - 42 • Guide staff/student use of identifiable photographs, referencing Release of Student  
43 Information.
  - 44 • Follow the Children’s Online Privacy Protection Act ([COPPA](#)) guidelines when using  
45 digital tools in the classroom.

- 1 • Provide age-appropriate instruction to students regarding appropriate online behavior.  
2 Such instruction shall include, but is not limited to: positive interactions with others  
3 online, including on social networking sites, and in chat rooms; proper online social  
4 etiquette; protection from online predators and personal safety; and how to recognize  
5 and respond to cyberbullying and other threats.
- 6 • Submit a Request for Software/App Review form when seeking to use new software or  
7 apps. Approval from the Director of Information Technology must be received before  
8 using. If needed, a Data Privacy Agreement must be completed and signed by authorized  
9 Great Falls Public Schools personnel and the software vendor as required by MCA 20-7-  
10 1323-1326.

### 11 Superintendent or designee Responsibilities

12 The Superintendent or designee will provide support to staff in following the Staff Technology  
13 Acceptable Use and Internet Safety Agreement. The Superintendent or designee will:

- 14 • Address staff infractions of the Staff Technology Acceptable Use and Safety Agreement  
15 according to District discipline policy.
- 16 • Maintain an updated list of students and staff who do not have permission to use the  
17 Internet, to use particular digital tools, to take technology home, or to have works or  
18 images displayed online.
- 19 • Notify the Informational Technology (IT) department whenever changes occur.

### 20 District Responsibilities

21 The District will provide support to staff and students in following the Staff Technology  
22 Acceptable Use and Internet Safety Agreement. The District will:

- 23 • Ensure that Children’s Internet Protection Act ([CIPA](#))-compliant filtering technology is  
24 in use.
- 25 • Review the Staff and Student Technology Acceptable Use Agreements as necessary.
- 26 • Establish procedures for an annual review of this policy by staff.
- 27 • Provide professional development for staff regarding expected behavior concerning  
28 this agreement.
- 29 • Ensure curriculum reflects digital citizenship.
- 30 • Monitors Internet activity and provides Internet usage reports to the Superintendent or  
31 designee for possible disciplinary action.
- 32 • Reviews new requests for software/apps and ensures Data Privacy Agreements are  
33 completed as required by MCA 20-7-1323-1326.

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

35 Staff may bring their own personal electronic devices which may or may not be able to connect  
36 to the District/school wireless network. When using personal electronic devices on school  
37 premises, staff must abide by the Staff Technology Acceptable Use and Safety Agreement. In  
38 addition, staff will:  
39  
40  
41  
42  
43  
44  
45  
46

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46

- Use personal devices for instruction only with the Superintendent or designees express permission. Students are not allowed to use personal devices supplied by staff.
- Only connect to the District/school wireless guest network and NOT to the District/school wired network. Staff understands 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 the device while connected to the District/school wireless network.
- Understand the security, care, and maintenance of their device as it is the staff member’s sole responsibility.
- Understand that the District/school is not responsible for the loss, theft, or damage of personal devices. Staff are fully responsible for their property while at school.
- Understand the Information Technology Department will not provide support for personal devices. Staff 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, then the staff member will need to use a device that is provided by the District/school to prevent any interruption to instruction and learning.
- Understand that staff are strictly prohibited from installing any device that directly interfaces with the District network including hubs, switches, routers, wireless access points, etc. These devices will be removed, if found, and the Superintendent or designee will be notified for potential disciplinary action. Personal peripheral equipment such as printers and scanners will only be permitted with the Superintendent or designee and the Director of Information Technology’s approval. Cameras and other USB devices present security concerns and should be used on a limited basis and for non-confidential purposes.

Failure to Follow Acceptable Use Agreement

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

Acceptance and Signature

I acknowledge and agree with the above guidelines, expectations, and responsibilities.

Staff Name (print) \_\_\_\_\_

Staff Signature \_\_\_\_\_ Date \_\_\_\_\_

Cross References:

- Policy 3225 Sexual Harassment/Intimidation of Students
- Policy 3226 Hazing, Harassment, Intimidation, Bullying

1	Policy 3231	Searches and Seizure
2	Policy 3300	Corrective Actions and Punishments
3	Policy 3310	Student Discipline
4	Policy 3630	Cellular Telephone and Electronic Signaling Device Policy
5	Policy 3612	District-Provided Access to Electronic Information, Services, and
6		Networks
7	Policy 5224	Political Activity – Staff Participation
8	Policy 5450	Employee Electronic Mail and Online Services Usage
9	Policy 5460	Electronic Resources and Social Networking
10	Policy 8320	Property Damage

11  
12 Legal References:

13	Family Educational Rights and Privacy Act ( <a href="#">FERPA</a> )	
14	Children’s Online Privacy Protection Act ( <a href="#">COPPA</a> )	
15	Children’s Internet Protection Act ( <a href="#">CIPA</a> )	
16	§ 20-7-1317, MCA	Electronic Directory Photograph Repository – Use in Search for
17		Missing Child Only – Annual Opt-In Notice Required
18	§ 20-7-1323-1326, MCA	Montana Pupil Online Personal Information Protection Act

19  
20 Policy History:

21	Adopted on:	November 26, 2007
22	Revised on:	February 12, 2018
23	Revised on:	August 22, 2022
24	Revised on:	May 11, 2026