Great Falls School District

PERSONNEL 5450F

Staff Computer Acceptable Use and Internet Safety Agreement

Great Falls Public Schools offers our staff access to the Internet and other electronic networks. It is important to remember that access is a privilege, not a right, and carries with it responsibilities of digital citizenship for all involved. Inappropriate use will result in cancellation of those privileges. The system administrator and/or principal will make all decisions regarding whether or not a user has violated these procedures and may monitor, deny, revoke, or suspend access at any time.

Terms of Agreement

In order for a staff member to obtain access to a school district electronic device, network, and the Internet, the staff member must sign an Acceptable Use Form at time of employment. The signed consent form is kept in their employee file. Thereafter, staff will be electronically prompted to review and accept this policy when they change their password annually.

Staff Acceptable Uses

The District provides electronic information, services, and networks for 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 staff on the Internet shall include but may not be limited to the following:

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

and/or pornography will face disciplinary action that may result in immediate termination. Users will report to immediate supervisor, any inadvertently accessed unsuitable material immediately.

- All use of telecommunication services or networks for the promotion of an individual's personal or political agenda or commercial initiatives are prohibited.
- Use of or engaging in offensive or inflammatory speech, profanity, or obscene language is not permitted at any time.
- Hate mail, harassment, discriminatory remarks, and other antisocial behaviors are not permitted.
- Users will not intentionally download unauthorized software, spread computer viruses, vandalize the data, infiltrate systems, damage hardware or software, or in any way degrade or disrupt the use of the network. If staff believes their computer is compromised, they should report it to the IT Help Desk immediately. Hacking or gaining unauthorized access to files, resources, or entities is prohibited.
- Users will follow confidentiality procedures when accessing personal information about students or employees and only release confidential information with proper authorization and consent per Family Educational Rights and Privacy Act (FERPA) regulations. Invading the privacy of individuals, which includes the unauthorized disclosure, dissemination, and use of information of a personal nature about anyone is prohibited.
- Users will maintain professional standards of behavior as detailed in the Professional Educators of Montana Code of Ethics and Board Policy 5460 which details the use of social networking.
- The District reserves the right to monitor, inspect, backup, review, and store at any time and without prior notice any and all usage of the school District network and Internet access, and all information transmitted or received in connection with such usage. This also includes any information stored on the school District network or local electronic devices. All such information will be and remain accessible by the District, and no staff will have any expectation of privacy regarding such information. Staff are advised that all material in whatever form in the school District, network may be considered public record pursuant to MCA 2-6-102.
- Publishing student pictures and work on websites can promote learning and collaboration, and provide an opportunity to share the achievements of students. If parents/guardians do not want release of student directory information, including photos and school work, schools must be notified in writing (see Student Handbook). Staff are responsible for checking student files for parental directives before posting student work online. For any student work to be published, the student and parent/guardian must sign a release.
- It is the responsibility of each staff member to treat the physical and digital property of others with respect. This includes proper treatment of digital devices and other hardware, the network system, and others' electronic files. Staff are not to remove, add or modify software, computer hardware or network equipment without prior Informational Technology Department authorization.
- 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 is not permitted per Board Policy 5224 Political

Activity – Staff Participation.

- Posting anonymous messages is not permitted.
- Staff will not use the network while access privileges are suspended or revoked.

Staff Responsibilities for Student Compliance. Staff are responsible for ensuring student compliance with the District's guidelines and expectations as listed below. Therefore, staff is responsible for understanding these guidelines and expectations.

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

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 networks, computers 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 spreading false information).
- 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 the network or the Internet.
- Uses that cause the uploading of a worm, virus, other harmful form of programming or vandalism.
- Uses that are "hacking" or any form of unauthorized access to other computers, networks, or other information.
- Uses that jeopardize the security of student access and of the computer network or other networks on the Internet.
- Uses that promote a personal commercial enterprise 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 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:

- 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.
- Students should log off District devices when 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 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 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 creation of 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. Such damage includes but is not limited to that cause by drops, spills, virus, exposure to heat and cold, or submersion.

Copyright Web Publishing Rules. Copyright law and District policy prohibit the republishing of text or graphics found on the Web or on District Websites of 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.
- Students should be polite and use appropriate language.

Teacher Responsibilities

Teachers will support students in their access to 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 students when they are accessing the Internet.
- Address student infractions of the Student Computer 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 Privacy 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.

Principal Responsibilities

Principals will provide support to teachers in following the staff Computer Acceptable Use and Internet Safety Agreement. Principals will:

- Address staff infractions of the Acceptable Use Agreement according to District discipline policy.
- Provide an updated list of students to teachers 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.

District Responsibilities

The District will provide support to principals, teachers, and students in following the Staff 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 Computer Acceptable Use Agreements as necessary.
- Establish procedures for an annual review of this policy by staff.
- 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

Staff 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 on school premises, staff must abide by the Staff Computer Acceptable Use Agreement. In addition, staff will:

- Use personal devices for instruction only with the Principal's 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 staff 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 school Principal will be notified for potential disciplinary action. Personal peripheral equipment such as printers, and scanners will only be permitted with Principal and Director of Information Technology 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's electronic devices, network, and the Internet 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
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, Services, and Networks

Policy 5224 Political Activity – Staff Participation
Policy 5450 Employee Electronic Mail and Online Services Usage
Policy 5460 Electronic Resources and Social Networking
Policy 8320 Property Damage

Legal References:
Family Educational Rights and Privacy Act (FERPA)
Children's Online Privacy Protection Act (COPPA)
Children's Internet Protection Act (CIPA)
20-7-1323-1326 Montana Pupil Online Personal Information Protection Act

Policy History:
Adopted on: November 26, 2007
Revised on: February 12, 2018
Revised on: August 22, 2022