Staff Use of the Internet, Electronic Communication and Technology

The Internet and electronic communications (e-mail, chat rooms, videos, blogs, social media and other forms of electronic communication) have vast potential to support curriculum and learning. The District believes they should be used in schools as a learning resource to educate and to inform. They should also be used to help the organization run more efficiently to meet District goals.

The District supports the use of the Internet and electronic communications by staff to improve teaching and learning through interpersonal communication, access to information, research, training, and collaboration and dissemination of successful educational practices, methods, and materials.

The Internet and electronic communications are fluid environments in which users may access materials and information from many sources. Staff members shall take responsibility for their own use of District computers and computer systems to avoid contact with material or information that violates this policy.

Internet Filtering

To protect students from child pornography or material and information that are obscene or harmful to minors, Internet filtering appliances that block or filter such material and information have been installed on the District network. All Internet usage is forced through these filters. Blocking or filtering is generally waived for a supervising teacher or school administrator, as necessary, and only after the teacher or administrator acknowledges a warning from the system for purposes of bona fide research or other educational projects being conducted by staff members over the age of 18. Such filtering is required by law under the Children's Internet Protection Act (CIPA, 2000).

Unauthorized and Acceptable Uses

Staff members shall use District technology equipment and technology systems in a responsible, efficient, ethical, and legal manner. Staff use of the network is a privilege, not a right.

Because technology and ways of using technology are constantly evolving, every unacceptable use of District computers and computer systems cannot be specifically described in policy. Therefore, examples of unacceptable uses include, but are not limited to, the following:

- Violation of respectful workplace standards
- Engagement in illegal behaviors
- Conducting personal commercial business
- Using District email addresses for personal profit or business
- Disrespect of a class or classes of individuals
- Excessive engagement in leisure activities during work hours
- Demeaning of the District, District personnel or students
- Purposefully accessing, creating, transmitting, retransmitting or forwarding of material or information:
o that promotes violence or advocates destruction of property including, but not limited to, access to information concerning the manufacturing or purchasing of destructive devices or weapons
o that contains pornographic, obscene, or other sexually oriented materials through either pictures or writings, that are intended to stimulate erotic feelings or appeal to prurient interests in nudity, sex, or excretion
o that plagiarizes the work of another without express consent
o that uses inappropriate or profane language likely to be offensive to others in the school community
o that is knowingly false or could be construed as intending to purposely damage another person’s reputation in violation of any federal or state law including but not limited to copyrighted material and material protected by trade secret
o that contains personal information about themselves or others, including information protected by confidentiality laws using another individual’s Internet or electronic communications account without written permission from that individual
o that impersonates another or transmits through an anonymous remailer
o that accesses fee services without specific permission from the system administrator

The District reserves the right, at its sole discretion, to determine the appropriateness of all information accessed through its technology.

Security

Security on District computer systems is a high priority. Staff members who identify a security problem while using the Internet or electronic communications must immediately notify a system administrator. Staff members should not demonstrate the problem to other users. Logging on to the Internet or electronic communications as a system administrator is prohibited except by those IT staff members whose job require such logging on.

Staff member must:

• Lock their machine any time they walk away, no matter how long it will be.

Staff members shall not:

• Use another employees’ password or any other identifier.
• Write down any passwords or post passwords, including sticky notes on monitors, desks, or any unsecure area.
• Log into any system not assigned to them, unless the system is designated as a public or multi-user machine.
• Gain or attempt to gain unauthorized access to District computers or computer systems.
• Read, alter, delete or copy electronic communications of other staff members.
• Place electronic devices of any kind on the District Network that are not authorized by the Director of Technology. Generally, this means that only District configured PCs, laptops and other personal network devices can be attached with a hardwire to the District Network.

Any staff member identified as a security risk, or as having a history of problems with other computer systems, may be denied access to the Internet and electronic communications.

Use of Social Media

Staff members are expected to serve as positive role models at all times and must represent their school and District professionally at all times. All off-campus expression on social media that is made pursuant to a staff member’s official job duties is subject to this policy.

Staff may not use a personal social media account to interact with students. If staff chooses to use social media to communicate with students, they should establish a separate public professional social media account. Staff members shall not use email, text messaging, instant messaging, or social networking sites to discuss non-school related issues with students. Staff members are expected to protect the health, safety, and emotional well-being of students and to preserve the integrity of the learning environment. Online or electronic conduct that distracts or disrupts the learning environment or other conduct in violation of this or related District policies may form the basis for disciplinary action up to and including dismissal from employment.

Vandalism

Vandalism will result in cancellation of privileges and may result in disciplinary action and/or legal action. Vandalism is defined as any malicious or intentional attempt to harm, destroy, modify, abuse, or disrupt:

• Operation of any network within the School District or any network connected to the Internet
• Operation of any form of electronic communications
• Data contained on any network or electronic communications
• Data of another user
• Usage by another user
• District-owned software or hardware
This includes, but is not limited to, the uploading or creation of computer viruses.

Unauthorized Software

Staff members are prohibited from using or possessing any software that has been downloaded or is otherwise in the user’s possession without appropriate registration and payment of any fees owed to the software owner. Licenses must be purchased for each device or each site per the requirements set forth by the software owner. All software must be used in accordance with the End-User License Agreement that accompanies any piece of software.

Unauthorized software shall include “free” software that is meant for individual, private use.

Instructional Use of Audio Visual Resources

All instructional resources, including audiovisual materials, must:

- Be consistent with Harrison School Board and District policies, educational goals, and the objectives of specific courses and/or activities
- Adhere to federal and state copyright laws
- Reflect the best teaching practices based on age appropriateness and instructional relevance

Movies and Movie Clips

Showing movies in class, as opposed to movie clips, should be a rare event in the Harrison School District. A teacher must obtain the permission of the Principal before showing a film in class that runs beyond twenty (20) minutes. Teachers may show YouTube and other streaming video clips in class as long as they reflect the best teaching practices as described above.

R-rated movies will be restricted to high school classes and then only with documented ties to the District curriculum, with approval from the school Principal and with written parental permission from each student who will view the movie or segments of the movie. When R-rated movies are to be shown in class high quality alternatives must be available for those for whom parental permission is not given or for whom watching the movie is a violation of personal conscience.

Streaming Services

Streaming services, such as Netflix, Amazon Instant Video, and Xfinity are meant for personal use only. It is against these companies’ terms of use to show any content in a public or shared setting including the classroom.

Staff Member Use is a Privilege

Use of the Internet and electronic communications requires personal responsibility and an understanding of the acceptable and unacceptable uses of such tools. Staff member use of the Internet and electronic communications is a privilege, not a right. Failure to follow the use procedures contained in this policy may result in the loss of the privilege to use these tools, restitution for costs associated with damages, and may result in school disciplinary action and/or legal action. The District may deny, revoke, or suspend access to District technology or close accounts at any time.

Each new employee will be required to sign the District’s Acceptable Use Agreement at New Employee Orientation. Once that form has been signed, network accounts will be issued. Additionally, staff members will be required to re-sign this agreement annually.

Employee Data

Staff Accounts

The District provides a network account for each staff member to access computers. These accounts are created during the night after an E-Pan has processed. Each staff member is also given an account in Office 365 (for email and Office access) and Google Apps. Upon receiving a termination E-pan, these accounts are promptly removed. Data in the user’s home folder is saved off for at least 30 days. E-mail data is immediately deleted from Office 365, but is recoverable up to 30 days after the account is deleted. Google accounts are deleted immediately. Data is recoverable for up to 5 days after the account is deleted. Human Capital may request a hold be placed on an account within this timeframe to prevent deletion.

Archiving of Electronic Email

District uses Exchange Online for email. 50GB of e-mail storage is provided to each user. Microsoft is responsible for maintaining backups to be used in the event of a catastrophic failure. District staff will be responsible to retain email related to the business of the District for a minimum of thirty (30) days on the District Email System (Colorado State Archive, Colorado School District Records Management, Schedule 2, item 9). Users may restore a deleted message from their Deleted Items folder for 30 days. After
messages are removed from Deleted Items, they can be restored by Technology for another 14 days. After a maximum of 45 days, the messages will no longer be recoverable. Users will only archive on District servers such email as specifically and purposefully needs to be archived consistently with the archive of “General Administrative Records” as described in Colorado State Archive, Colorado School District Records Management, Schedule 2.

User Storage

The Technology Department will diligently attempt to provide two (2) weeks of backups for the home directories of users for at least 1GB of files and folders. Special permission must be obtained from the Executive Director of Technology for users requiring more than 1GB of backed up space in a user’s home directory. Files stored in the home directory must be related to District business. Up to 1TB of storage is also available through Office 365 (OneDrive).

Confidentiality

Staff members shall not access, receive, transmit, or retransmit material regarding students, parents/guardians, or District employees that is protected by confidentiality laws unless such access, receipt or transmittal is in accordance with their assigned job responsibilities, applicable law, and District policy. If material is not legally protected, but is of a confidential or sensitive nature, great care shall be taken to ensure that only those with a "need to know" are allowed access to the material. Staff members shall handle all employee, student, and District records in accordance with policies GBP (Personnel Records and Files), JRA/JRC (Student Records/Release of Information on Students), and EGAEE (Public Electronic Communication Records).

Disclosure of confidential student records, including disclosure via electronic mail or other telecommunication systems, is governed by state and federal law, including the Family Educational Rights and Privacy Act (FERPA), Children’s Online Privacy Protection Rule (COPPA), and Colorado House Bill 16-1423 – Student Data Transparency and Security Act. (See policy JRA/JRC/1CRR, Student Records/Release of Information on Students and Privacy and Protection of Confidential Student Information for detailed information on student records).

It is imperative that staff members who share confidential student information via electronic communications understand the correct use of technology, so that confidential records are not inadvertently sent or forwarded to the wrong party. Staff members who use e-mail to disclose student records or other confidential student information in a manner inconsistent with applicable law and District policy may be subject to disciplinary action.

Privacy Expectations

District computers and computer systems are owned by the District and are intended for educational purposes and District business at all times. Staff members shall have no expectation of privacy when using the Internet or electronic communications. The District reserves the right to monitor, inspect, copy, review, and store (at any time and without prior notice) all usage of District computers and computer systems, including all Internet and electronic communications access and transmission/receipt of materials and information. All material and information accessed/received through District computers and computer systems shall remain the property of the District.

Public Records

Electronic communications sent and received by District employees may be considered a public record subject to public disclosure or inspection under the Colorado Open Records Act. All employee electronic communications shall be monitored to ensure that all public electronic communication records are retained, archived, and destroyed in accordance with applicable law or policy.

Equipment

Cellular Phones

District cell phones are intended for District business which includes calls, e-mail, apps, texting, Internet use, and any other data. If you use your work cell for personal use, it is subject to auditing under the Colorado Open Records ACT (CORA). The District cannot be held responsible for any loss of data on District cellphone. Any additional fees incurred by the employee may need to be paid for by the employee. Types of these additional fees include but are not limited to: 411 calls; paid apps; international calls, texting, e-mail, or data; and premium-rate telephone numbers.

Employees may not pay to keep their District cell phone under any circumstances. Phone numbers will also stay with the position and cannot be ported to the employee’s personal carrier. All accessories that came with the equipment (including the box) need to be kept in case the device has to be returned for warranty replacement. Any accessories that are not included when the device is returned will need to be replaced at the employee’s cost. Employees will not attempt to physically alter or attempt to repair the District cellular phone. Employees shall not take a broken device to a third party company to repair the device as this will void the warranty.

Computers and Tablets
District computers and tablets are intended for District business only including Internet use, software, apps, and any other data. Employees will not attempt to physically alter or attempt to repair computers or tablets. Any accessories not included with the computer or tablet when the device is turned in will need to be replaced at the employee’s expense.

**Other Equipment**

All other technology equipment needs to be approved by Technology before it can be used in the District. Any unapproved Technology will not be supported and will be removed and may result in disciplinary or legal action. Unmanaged switches (*dumb* switches) are not allowed on the network as they are a security risk and they degrade performance and in some instances take an entire network down.

**School District Makes No Warranties**

The District makes no warranties of any kind, whether expressed or implied, related to the use of District computers and computer systems, including access to the Internet and electronic communications services. Providing access to these services does not imply endorsement by the District of the content, nor does the District make any guarantee as to the accuracy or quality of information received. The District is not responsible for any damages, losses, or costs a staff member encounters in using the Internet and electronic communications. This includes loss of data and service interruptions. Use of any information obtained via the Internet and electronic communications is at the staff member’s own risk.

---

**Legal**

47 U.S.C. 201 et seq. *(Communications Decency Act of 1995)*

The Family Educational Rights and Privacy Act (FERPA) (20 U.S.C. § 1232g; 34 CFR Part 99)


Student Data Transparency and security Act ("Act") HB 16-1423 - Colorado Revised Statutes § 22-16-101 et seq.

---

**Legal**

47 U.S.C. 201 et seq. *(Communications Decency Act of 1995)*