# Henry County R-1 Technology Guide 2025-2026



#### General Information

Our district employs a Technology Director/Network Administrator and one technology assistant. The Technology Director is responsible for the District's overall technology footprint (Network security, servers, connections, COPPA, FERPA and CIPA compliance, and budgetary compliance). The Technology Assistant is responsible for solving user issues, repairs, maintaining current documentation for audit compliance, among others. The Henry County R- I School District has placed great emphasis on technology use and integration.

It is required by our district that employees, students, and parents/guardians sign User Agreements. User Agreements put employees, students, and parents/guardians on notice that any information stored or transmitted using district technology is not private and may be monitored or searched by district Administration. They also provide evidence that the student, parent/guardian, and employee is aware of the district rules regarding usage and accepts responsibility for any damage he or she causes the district's technology. They must be signed and returned before access is given to district technology. All technology purchases must go through the Technology Department for review to ensure compatibility with our current infrastructure.

All technology used by students and staff is for **educational purposes**. Great amounts of district, state, and federal monies were spent for this use. It is not to be misused or abused.

Any teacher utilizing a Chromebook for instructional purposes must be present at all times and move throughout the room during student use to ensure proper and safe utilization of district technology. The teacher is not to rely on the technology staff to monitor student behavior when using district technology with students.

Questions regarding 1:1 behavior issues should be turned into building Principals. Students who forget their device, or bring it uncharged, will be addressed following District policy. If a teacher sees something wrong with a 1:1 device, please have the student report the incident to the school building office to ensure the device is fixed in a proper manner and process. Other questions may be referred to the Technology Assistant and/or Technology Director.

Every teacher has a file (user folder) on the school's server. It is recommended that you save your important educational files there or on your Google Drive, so that they will not be lost if your computer should crash. Do not save to the "My Documents" area or the local computer if you do not want to lose it. When saving to the server, you can open that file anywhere in the district when logged in as you. This is handy when you want to open the file in the computer lab, on your classroom computer or in a different building. Please do not save personal pictures or videos on the server. (They will be deleted) Every teacher also has a school district Google Drive that can be utilized to store documents. The server drive space will be evaluated once a quarter for usage per user and you may be asked to move some data off to an external drive.

### Trouble Shooting

It is inevitable that you will probably have computer problems or issues at some point in time! If you are having a problem, there are basic steps you can personally follow before creating a ticket. The first step is always to restart your machine. You can also ensure your network cord is connected properly or seeing if others are having the same problem (building/districtwide issue). If the problem cannot be resolved through these means, then you will need to submit a ticket and the Technology department will help identify your problem. Creating a ticket is easy, simply email <a href="tech@henrycountyr1.k12.mo.us">tech@henrycountyr1.k12.mo.us</a> for Tech requests, or <a href="maintenance@henrycountyr1.k12.mo.us">maintenance@henrycountyr1.k12.mo.us</a> for Maintenance requests.

Please keep in mind that your requests are important to us. However, we must follow protocol in order to ensure that everything is taken care of in a first in/first out order. Understand that some technology problems can be fixed quickly, while others take some time. District-wide technology issues take precedence over individual issues that arise. This could cause district technology staff to delay in working on your technology problem. We will do our best to serve you, while serving the district as a whole.

# Henry County R-1 School District Email System

Conditions and Guidelines of Use

All student and staff Electronic Mail (email) as well as Google and Network drive accounts are property of the Henry County R-1 School District.

The primary purpose of the student/staff electronic mail system is for students to communicate with school staff, outside resources, related school assignments and projects within limits set by the district, and fellow students to collaborate on school assignments and projects. Use of the district's email system is a privilege.

The user will be removed from the system after graduation, or leaving the school district.

Use of the email system will align with the school's code of conduct/discipline policy and the code/discipline policy will be used for discipline purposes. Communication through the district's email system will exhibit common sense and civility. It will abide by the community's mode of acceptable behavior. Users are responsible for messages sent from their accounts.

Users should not share their usernames and/or passwords.

All users must adhere to the same standards for communicating electronically that are expected in the classroom and that are consistent with district policies and procedures.

When communicating electronically, all users must comply with district policies, regulations and procedures and adhere to the same standards expected in the classroom. All staff users are required to participate in monthly security training.

Messages posted on the district's email system cannot cause disruption to the school environment or normal and acceptable school operations (including, but not limited to spam" communications, messages of a bullying/harassing nature, obscene email, attempts by adults to lure them into dangerous behaviors, and the like).

The email system cannot be used to operate a personal business.

Users will not identify their home telephone numbers, or home addresses in any email correspondence.

Users will report any unusual activities such as "spam" communications, messages of a bullying/harassing nature, obscene email, attempts by adults to lure them into dangerous behaviors, and the like to the school's technology department for action. Users should not forward chain letters, jokes, or graphics files.

Electronic mail sent or received by the email system is not confidential. Although the Board of Education does not make a practice of monitoring electronic mail, the administration reserves the right to filter and retrieve the contents of user mailboxes for legitimate reasons, such as to find lost messages, to conduct

internal investigations, to comply with investigations of wrongful acts or to recover from system failure.

System administrators may create filters to scan for and eliminate viruses and large graphic files that are unrelated to the school district's operation or email not meeting the Child Internet Protection Act (CIPA) regulations (e.g. "spam" communications, obscene email, attempts by adults to lure students into dangerous behaviors, and the like).

Improper use of the system will result in discipline and possible revocation of the user's network and/or E-mail account. Illegal activities on the system will be referred to law enforcement authorities for appropriate legal action.

# Henry County R-1 School District

## Technology Usage

The Henry County R-I School District's technology exists for the purpose of enhancing the educational opportunities and achievement of district students. Research shows that students who have access to technology improve achievement. In addition, technology assists with the professional enrichment of the staff and increases engagement of students' families and other patrons of the district, all of which positively impact student achievement. The district will periodically conduct a technology census to ensure that instructional resources and equipment that support and extend the curriculum are readily available to teachers and students.

The purpose of this policy is to facilitate access to district technology and to create a safe environment in which to use that technology. Because technology changes rapidly and employees and students need immediate guidance, the superintendent or designee is directed to create procedures to implement this policy and to regularly review those procedures to ensure they are current.

#### Definitions

For the purposes of this policy and related procedures and forms, the following terms are defined:

Technology Resources - Technologies, devices and services used to access, process, store or communicate information. This definition includes, but is not limited to: computers; modems; printers; scanners; fax machines and transmissions; telephonic equipment; mobile phones; audio-visual equipment; Internet; electronic mail (e-mail); electronic communications devices and services, including wireless access; multimedia resources; hardware; and software. Technology resources may include technologies, devices and services provided to the district by a third party.

User - Any person who is permitted by the district to utilize any portion of the district's technology resources including, but not limited to, students, employees, School Board members and agents of the school district. User Identification (ID) - Any identifier that would allow a user access to the district's technology resources or to any program including, but not limited to, e-mail and Internet access.

Password - A unique word, phrase or combination of alphabetic, numeric and non-alphanumeric characters used to authenticate a user ID as belonging to a user.

#### Authorized Users

The district's technology resources may be used by authorized students, employees, School Board members and other persons approved by the superintendent or designee, such as consultants, legal counsel and independent contractors. All users must agree to follow the district's policies and procedures and sign or electronically consent to the district's User Agreement prior to accessing or using district technology resources, unless excused by the superintendent or designee.

Use of the district's technology resources is a privilege, not a right. No potential user will be given an ID, password, or other access to district technology if he or she is considered a security risk by the superintendent or designee.

#### User Privacy

A user does not have a legal expectation of privacy in the user's electronic communications or other activities involving the district's technology resources including, but not limited to, voice mail, telecommunications, e-mail and access to the Internet or network drives. By using the district's network and technology resources, all users are consenting to having their electronic communications and all other use monitored by the district. A user ID with e-mail access will only be provided to authorized users on condition that the user consents to interception of or access to all communications accessed, sent, received or stored using district technology.

Electronic communications, downloaded material and all data stored on the district's technology resources, including files deleted from a user's account, may be intercepted, accessed, monitored or searched by district administrators or their designees at any time in the regular course of business. Such access may include, but is not limited to, verifying that users are complying with district policies and rules and investigating potential misconduct. Any such search, access or interception shall comply with all applicable laws. Users are required to return district technology resources to the district upon demand including, but not limited to, mobile phones, laptops and tablets.

#### Technology Administration

The Board directs the superintendent or designee to assign trained personnel to maintain the district's technology in a manner that will protect the district from liability and will protect confidential student and employee information retained on or accessible through district technology resources.

Administrators of district technology resources may suspend access to and/or availability of the district's technology resources to diagnose and investigate network problems or potential violations of the law or district policies and procedures. All district technology resources are considered district property. The district may remove, change or exchange

hardware or other technology between buildings, classrooms or users at any time without prior notice. Authorized district personnel may install or remove programs or information, install equipment, upgrade any system or enter any system at any time.

#### Content Filtering and Monitoring

The district will monitor the online activities of minors and operate a technology protection measure ("content filter") on the network and all district technology with Internet access, as required by law. In accordance with law, the content filter will be used to protect against access to visual depictions that are obscene or harmful to minors or are child pornography. Content filters are not foolproof, and the district cannot guarantee that users will never be able to access offensive materials using district equipment. Evading or disabling, or attempting to evade or disable, a content filter installed by the district is prohibited.

The superintendent, designee or the district's technology administrator may fully or partially disable the district's content filter to enable access for an adult for bona fide research or other lawful purposes. In making decisions to fully or partially disable the district's content filter, the administrator shall consider whether the use will serve a legitimate educational purpose or otherwise benefit the district.

The superintendent or designee will create a procedure that allows students, employees or other users to request that the district review or adjust the content filter to allow access to a website or specific content.

#### Online Safety, Security and Confidentiality

In addition to the use of a content filter, the district will take measures to prevent minors from using district technology to access inappropriate matter or materials harmful to minors on the Internet. Such measures shall include, but are not limited to, supervising and monitoring student technology use, careful planning when using technology in the curriculum, and instruction on appropriate materials. The superintendent, designee and/or the district's technology administrator will develop procedures to provide users guidance on which materials and uses are inappropriate, including network etiquette guidelines.

All minor students will be instructed on safety and security issues, including instruction on the dangers of sharing personal information about themselves or others when using e-mail, social media, chat rooms or other forms of direct electronic communication. Instruction will also address cyberbullying awareness and response and appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms.

This instruction will occur in the district's computer courses, courses in which students are introduced to the computer and the Internet, or courses that use the Internet in instruction. Students are required to follow all district rules when using district technology resources and are prohibited from sharing personal information online unless authorized by the district.

All district employees must abide by state and federal law and Board policies and procedures when using district technology resources to communicate information about personally identifiable students to prevent unlawful disclosure of student information or records.

All users are prohibited from using district technology to gain unauthorized access to a technology system or information; connect to other systems in evasion of the physical limitations of the remote system; copy district files without authorization; interfere with the ability of others to utilize technology; secure a higher level of privilege without authorization; introduce computer viruses, hacking tools, or other disruptive/destructive programs onto district technology; or evade or disable a content filter.

#### Closed Forum

The district's technology resources are not a public forum for expression of any kind and are to be considered a closed forum to the extent allowed by law. The district's webpage will provide information about the school district, but will not be used as an open forum.

All expressive activities involving district technology resources that students, parents/guardians and members of the public might reasonably perceive to bear the imprimatur of the district and that are designed to impart particular knowledge or skills to student participants and audiences are considered curricular publications. All curricular publications are subject to reasonable prior restraint, editing and deletion on behalf of the school district for legitimate pedagogical reasons. All other expressive activities involving the district's technology are subject to reasonable prior restraint and subject matter restrictions as allowed by law and Board policies.

#### Inventory and Disposal

The district will regularly inventory all district technology resources in accordance with the district's policies on inventory management. Technology resources that are no longer needed will be disposed of in accordance with law and district policies and procedures related to disposal of surplus property.

#### Violations of Technology Usage Policies and Procedures

Use of technology resources in a disruptive, inappropriate or illegal manner impairs the district's mission, squanders resources and shall not be tolerated. Therefore, a consistently high level of personal

responsibility is expected of all users granted access to the district's technology resources. Any violation of district policies or procedures regarding technology usage may result in temporary, long-term or permanent suspension of user privileges. User privileges may be suspended pending investigation into the use of the district's technology resources.

Employees may be disciplined or terminated, and students suspended or expelled, for violating the district's technology policies and procedures. Any attempted violation of the district's technology policies or procedures, regardless of the success or failure of the attempt, may result in the same discipline or suspension of privileges as that of an actual violation. The district will cooperate with law enforcement in investigating any unlawful use of the district's technology resources.

#### Damages

All damages incurred by the district due to a user's intentional or negligent misuse of the district's technology resources, including loss of property and staff time, will be charged to the user. District administrators have the authority to sign any criminal complaint regarding damage to district technology.

#### No Warranty/No Endorsement

The district makes no warranties of any kind, whether expressed or implied, for the services, products or access it provides. The district's technology resources are available on an "as is, as available" basis.

The district is not responsible for loss of data, delays, non-deliveries, mis-deliveries or service interruptions. The district does not endorse the content nor guarantee the accuracy or quality of information obtained using the district's technology resources.

#### TECHNOLOGY USAGE

(Technology Safety)

#### Student Users

All student users and their parents/guardians must sign the district's User Agreement prior to accessing or using district technology resources, unless otherwise excused by this policy or the superintendent or designee. Students who are 18 or who are otherwise able to enter into an enforceable contract may sign or consent to the User Agreement without additional signatures. Students who do not have a User Agreement on file with the district may be granted permission to use the district's technology resources by the superintendent or designee.

#### Employee Users

No employee will be given access to the district's technology resources unless the employee agrees to follow the district's User Agreement prior to accessing or using the district's technology resources. Authorized employees may use the district's technology resources for reasonable, incidental personal purposes if the use does not violate any provision of district policies or procedures, hinder the use of the district's technology resources for the benefit of its students or waste district resources. Any use that jeopardizes the safety, security or usefulness of the district's technology resources or interferes with the effective and professional performance of the employee's job is considered unreasonable. Unless authorized by the employee's supervisor in advance, employees may not access, view, display, store, print or disseminate information using district technology resources that students or other users could not access, view, display, store, print or disseminate.

#### External Users

Consultants, legal counsel, independent contractors and other persons having business with the district may be granted user privileges at the discretion of the superintendent or designee after consenting to the district's User Agreement and for the sole, limited purpose of conducting business with the school. External users must abide by all laws, district policies and procedures.

#### General Rules and Responsibilities

The following rules and responsibilities will apply to all users of the district's technology resources:

- 1. Applying for a user ID under false pretenses or using another person's ID or password is prohibited.
- 2. Sharing user IDs or passwords with others is prohibited except when shared with the district's technology department for the purpose of

support. Individuals who share IDs or passwords may be disciplined and will be held responsible for any actions taken by those using the ID or password. A user will not be responsible for theft of passwords and IDs, but may be responsible if the theft was the result of user negligence.

- 3. Deleting, examining, copying or modifying district files or data without authorization is prohibited.
- 4. Deleting, examining, copying or modifying files or data belonging to other users without their prior consent is prohibited.
- 5. Mass consumption of technology resources that inhibits use by others is prohibited.
- 6. Use of district technology for soliciting, advertising, fundraising, commercial purposes or financial gain is prohibited, unless authorized by the Superintendent. Use of district technology resources to advocate, support or oppose any ballot measure or candidate for public office is prohibited.
- 7. Accessing fee services without permission from an administrator is prohibited. A user who accesses such services without permission is solely responsible for all charges incurred.
- 8. Users are required to obey all laws, including criminal, copyright, privacy, defamation and obscenity laws. The district will render all reasonable assistance to local, state or federal officials for the investigation and prosecution of persons using district technology in violation of any law.
- 9. The district prohibits the use of district technology resources to access, view or disseminate information that is pornographic, obscene, child pornography, harmful to minors, obscene to minors, libelous, or pervasively indecent or vulgar.
- 10. Accessing, viewing or disseminating information on any product or service not permitted to minors is prohibited unless under the direction and supervision of district staff for curriculum-related purposes.
- 11. The district prohibits the use of district technology resources to access, view or disseminate information that constitutes insulting or fighting words, the very expression of which injures or harasses other people (e.g., threats of violence, defamation of character or of a person's race, religion or ethnic origin); presents a clear and present likelihood that, because of their content or their manner of distribution, they will cause a material and substantial disruption of the proper and orderly operation and discipline of the school or school activities; or will cause the commission of unlawful acts or the violation of lawful district policies and procedures.
- 12. The district prohibits any use that violates any person's rights under applicable laws, and specifically prohibits any use that has the purpose or effect of discriminating against or harassing any person on the basis of race, color, religion, sex, national origin, ancestry, disability, age, genetic information, pregnancy or use of leave protected by the Family and Medical Leave Act (FMLA).
- 13. The district prohibits any unauthorized intentional or negligent action that damages or disrupts technology, alters its normal performance or

- causes it to malfunction. The district will hold users responsible for such damage and will seek both criminal and civil remedies, as necessary.
- 14. Users may install and use only properly licensed software and audio or video media purchased by the district or approved for use by the district. All users will adhere to the limitations of the district's technology licenses. Copying for home use is prohibited unless permitted by the district's license and approved by the district.
- 15. At no time will district technology or software be removed from district premises, unless authorized by the district.
- 16. All users will use the district's property as it was intended. Technology resources will not be moved or relocated without permission from a building administrator. All users will be held accountable for any damage they cause to district technology resources.

#### Technology Security and Unauthorized Access

- 1. All users shall immediately report any security problems or misuse of the district's technology resources to a teacher or administrator.
- Use of district technology resources in attempting to gain or gaining unauthorized access to any technology system or the files of another is prohibited.
- 3. Use of district technology to connect to other systems, in evasion of the physical limitations of the remote system, is prohibited.
- 4. The unauthorized copying of system files is prohibited.
- 5. Intentional or negligent attempts, whether successful or unsuccessful, to interfere with the ability of others to utilize any district technology are prohibited.
- 6. Users will be granted access privileges to district technology resources as determined appropriate by the superintendent or designee. Any attempt to secure a higher level of privilege without authorization is prohibited.
- 7. The introduction of computer viruses, hacking tools or other disruptive or destructive programs into a district computer, network or any external networks is prohibited.

#### Online Safety and Confidentiality

Curricular or noncurricular publications distributed using district technology will comply with the law and Board policies on confidentiality.

All district employees will abide by state and federal law, Board policies and district rules when using district technology resources to communicate information about personally identifiable students. Employees will take precautions to prevent negligent disclosure of student information or student records.

All students will be instructed on the dangers of sharing personal information about themselves or others over the Internet and are

prohibited from sharing such information unless authorized by the district. Student users shall not agree to meet with someone they have met online without parental approval and must promptly disclose to a teacher or another district employee any message the user receives that is inappropriate or makes the user feel uncomfortable.

#### Electronic Mail and Messaging

A user is generally responsible for all e-mail and other electronic messages originating from the user's accounts; however, users will not be held responsible when the messages originating from their accounts are the result of the account being hacked.

- 1. Forgery or attempted forgery of electronic messages is illegal and prohibited.
- 2. Unauthorized attempts to read, delete, copy or modify electronic messages of other users are prohibited.
- 3. All users must adhere to the same standards for communicating electronically that are expected in the classroom and that are consistent with district policies and procedures.
- 4. When communicating electronically, all users must comply with district policies, regulations and procedures and adhere to the same standards expected in the classroom.
- 5. Users must obtain permission from the superintendent or designee before sending any districtwide electronic messages.

#### Communication Devices

Employees and others to whom the district provides electronic communication devices must use them professionally and in accordance with district policies, regulations and procedures. These devices shall not be used in a manner that would distract the employee or other user from adequate supervision of students or other job duties.

#### Exceptions

Exceptions to district rules will be made for district employees or agents conducting an investigation of a use that potentially violates the law, district policies or procedures. Exceptions will also be made for technology administrators who need access to district technology resources to maintain the district's resources or examine and delete data stored on district computers as allowed by the district's retention policy.

#### Waiver

Any user who believes he or she has a legitimate educational purpose for using the district's technology in a manner that may violate any of the district's policies, regulations or procedures may request a waiver from the building principal, superintendent or their designees. In making the decision to grant a waiver to a student, the administrator shall consider the student's purpose, age, maturity and level of supervision involved.

#### STAFF USE OF COMMUNICATIONS DEVICES

The Henry County R-1 School District encourages district employees to use technology, including communication devices, to improve efficiency and safety. The district expects all employees to use communication devices in a responsible manner that does not interfere with the employee's job duties. Employees who violate district policies and procedures governing the use of communication devices may be disciplined, up to and including termination, and may be prohibited from possessing or using communication devices while at work. Communication devices may not be used in any manner that would violate the district's policy on student-staff relations.

#### Definitions

Communication Device - Any portable device that sends or receives calls or text messages allows the retrieval of e-mail or provides access to the Internet.

Use/Using - Answering the phone or talking on the phone; sending or responding to a text, e-mail or other communication; opening and viewing pictures or digital recordings; opening and listening to music or audio communications; continuously checking a communication device; or any activity with a communication device that interferes with the employee's job duties or appropriate supervision of students.

#### General Use

The district prohibits employees from using any communication device that interrupts or disrupts the performance of duties by the employee or otherwise interferes with district operations, as determined by the employee's supervisor. This prohibition applies regardless of whether the communication device used is owned by the employee or provided by the district.

Employees are responsible for keeping communication devices secure and, if possible, password protected.

Supervision of students is a priority in the district, and employees who are responsible for supervising students must always concentrate on that task. Employees shall not use communication devices when they are responsible for supervising students unless any of the following conditions occurs:

- 1. The device is being used to instruct the students being supervised at the time.
- 2. The use is necessary to the performance of an employment-related duty.
- 3. The employee has received specific and direct permission from a supervisor.
- 4. There is an emergency.

Even when these conditions exist, the employee is responsible for obtaining assistance in adequately supervising students during the approved use so that students are always supervised.

#### Social Media Guidelines for Faculty and Staff

Henry County R-1 School District realizes that part of learning is adapting to the changing methods of communication. The importance of faculty, staff, students, and parents engaging, collaborating, learning, and sharing in these digital environments is part of learning. To this aim, Henry County R-1 School District has developed the following guidelines to provide direction for employees, participating in online social media activities in their personal capacity (blogs, wikis, online social networks, application ["app"] development, or any other form of online publishing or discussion). While these guidelines may also be helpful for employees posting in their professional capacity, those postings are subject to board policy.

Free speech protects educators who want to participate in social media, but laws and courts have ruled that speech made pursuant to an employee's duties, as an employee of the district, are not fully protected by the First Amendment and schools can discipline faculty and staff if their speech, including online postings, disrupts school operations. Henry County R-1 social media guidelines encourage employees to participate in online social activities. However, it is important to create an atmosphere of trust and individual accountability; keeping in mind that information produced by Henry County R-1 School District faculty, staff, and students is a reflection on the entire district and is subject to the district's Acceptable Use Policy. By accessing, creating, or contributing to any blogs, wikis, apps, websites or other social media for classroom or

district use, you agree to abide by these guidelines. Please read them carefully before creating or participating in any online content.

Examples of social media include but are not limited to the following: blogs, X (Formerly Twitter), Facebook, LinkedIn, Instagram, YouTube, Google Sites and/or other website design tool, and the like, etc.

#### Be Transparent

• How you represent yourself online is an extension of yourself. It is recommended that you do not misrepresent yourself by using someone else's identity or misrepresenting your identity. Be honest about who you are, where you work, and what you do.

#### Personal Responsibility

- Henry County R-1 School District employees are personally responsible for the content they publish online. Be mindful that what you publish on your personal social media accounts will be public for a long time - it is recommended that you protect your privacy.
- Be aware that even with the strictest privacy settings what you 'say' online should be within the bounds of professional discretion. Comments expressed via social networking pages under the impression of a 'private conversation' may still end up being shared into a more public domain, even with privacy settings on maximum. Anyone can take a picture of what you say and share it with others without your knowledge.
- Your online behavior should reflect the same standards of honesty, respect, and consideration that you use face-to-face.
- Comments related to the school should always meet the highest standards of professional discretion even when commenting on personal social media accounts. When posting, even on the strictest settings, staff should act on the assumption that all postings are in the public domain.
- When contributing online, do not post confidential student information or to your personal accounts or "tag" them in a photo. This may include, but is not limited to student photos, names, grades, behavior, etc.
- Remember that online posts and content are an extension of your classroom or the workplace. What is inappropriate in your classroom or the workplace should be deemed inappropriate online.
- If you want to have a professional presence through social media that is not used for classroom or district use, developing a profile on a site like LinkedIn or something similar might be a great practice. Otherwise, it is important to state that "any thoughts shared are your own thoughts and not that of the district".

#### Always A School Employee

The lines between "public and private" & "personal and professional" are blurred in the digital world. Even when you have a disclaimer or use a different user name, you will always be considered a district employee. Whether it is clearly communicated or not and even if it is not your intent, you will be identified as working for and sometimes representing the school in what you do and say online.

When writing personal posts, it is recommended that you always write in the first person (I, me, we, us) and make it clear that you are speaking for yourself and not on behalf of the district.

#### Use a Disclaimer

- Include a disclaimer on your social media site which says something like this: "The opinions and positions expressed on this site are my own and do not necessarily reflect my school district's positions, strategies, or opinions."
- This standard disclaimer does not exempt employees from their responsibilities as explained in these guidelines that do fall under board policies.
- When in doubt, direct the public to the principal or superintendent.

#### Media Relations

If asked by media to comment on a school-related issue, please refer them to the Henry County R-1 School District Administrative Offices (660)647-3533. Please do not comment on behalf of the school district. When in doubt on how you should comment on social media, direct the public to your building principal or superintendent.

#### Be Respectful and Responsible

Employees, parents, and students reflect a diverse set of customs, values, and points of view. Be respectful of the opinions of others in your posts or comments. You are responsible for the content you post. Consider the words used to tag content in a social bookmarking site. Consider the profile picture or image you select. Do your tags, descriptions, and image portray you or others in the way you want to be portrayed?

#### Own and Correct Mistakes

If you make a mistake, admit the mistake and correct it quickly. Be sure to clearly state if you have corrected a previous post. Even

though damage may be done, it is best to admit your mistake and correct it. Apologize if appropriate.

#### Confidential Information

Online postings and conversations are not private. Do not share confidential information whether it is internal school discussions or specific information about students or other staff or school situations (including crisis events). What you post will be seen and possibly shared by others and will be online for a long time. It can be forwarded or shared in just a few clicks. Do no write about a colleague or student without their permission.

#### School Crisis Situations

During a school lockdown, secure mode, or crisis, employees should not be posting or asking for information online or through other forms of communication (texts, phone calls, etc.). During these situations, rumors can spread quickly and employees should be using this time to make sure that the safety of those in their charge/care is their top priority.

#### Posting Photos or Movies of Students and Staff

No photos should be posted if it would violate FERPA or HIPPA or identify a student as a special-needs student. This includes posting through online accounts, text messaging, or the physical posting of a photo in an employee's classroom or home (designated as special services).

No photos of activities to which the general public was not invited or not allowed may be posted on faculty and staff's personal social media accounts. However, these photos must be initially posted on a school or classroom, district-approved social media account and then shared from that account if the staff member wishes to share them on his/her personal social media. Please keep in mind you must have obtained parent permission for any photo, video, likeness, or work of the student.

There are situations of a personal nature in which you are a family member, friends with parents of a student, work with students in another capacity outside of school and have <u>parent permission to post on your personal social media account.</u> In those cases, your administrator should be made aware. Remember it is recommended to be transparent in your communications.

#### Using Content That Isn't Your Own

Do not utilize protected works. Just because an image, song, movie, etc. comes up in a search online does not mean you can use it freely. Documents found online should be available under Creative Commons or your own if you plan to reproduce them in any way. Also, make sure and give credit to the owner of the work when necessary.

A hyperlink to outside sources is recommended. Be sure not to plagiarize and give credit where it is due. When using a hyperlink, be sure that content is appropriate and adheres to the Henry County R-1 School District policies.

Creative Commons is a way that allows you to use certain photos without getting written permission from the owner. Check out https://creativecommons.org/about for more information.

#### Responding to Negative Comments and Criticism

How you respond to negative comments or criticism will say more about you and your character than what you post. If you delete a negative post, it discourages open communications. When publicly criticized or the recipient of a negative comment, first, stay cool/calm and do not reply in haste. Express your view in a clear and logical way. Do not get personal, and, if you made a mistake, admit it, and move ahead. It is not uncommon for a negative response to be answered by some other person, who supports your view. When in doubt, it is best to ignore a comment and not give it credibility by acknowledging it with a response publicly; perhaps a face-to-face meeting would be more appropriate.

When someone makes a negative comment or criticism on a district, school, classroom, or district-approved social media account be sure to keep in mind the commenting guidelines for District Facebook/social media pages.

#### Requests to Use Blocked Social Media Sites

The Henry County R-1 School District understands that technology and learning is constantly changing and that many sites currently "blocked" by the District's content filter may have pedagogical significance for teacher and student use.

If you would like to request another online site be accessible for teaching and learning, contact the District's Technology Director to review the website. Requests will be reviewed and, if approved, the district's content filter will be updated accordingly. A link to the sites privacy policy should be included if possible.

# Request to Start and Maintain a Social Media Account or Web Presence for A School Program/Activity/Sport

Henry County R-1 School District understands that having a social media presence for a school program, activity, or sport can be a great method of communication and a promotional tool.

Before a program, activity, or sport can start a social media presence, the building principal or superintendent must approve the account the staff member wishes to create. Employees should get a written and signed approval before creating the page.

Any social media account or Web presence that has been established prior to this procedure will still need to be approved by the superintendent). The building principal must be given administrative access. Any account not approved by the district but is deemed to represent or seem to represent the District in an official manner will result in the district pursuing removal of the account.