Hatch Valley Public Schools
Information & Communication Technologies
Acceptable Use Policy (AUP) & Guidelines

- **Introduction**

Hatch Valley Public Schools (HVPS) is pleased to provide its students and staff access to all of our current and future various Information & Communication Technologies (ICT). These district resources provide opportunities to enhance communication and learning in both our local and global communities. The privilege of access necessitates that each user act as a responsible digital citizen and follow the founding principles of the Children's Internet Protection Act (CIPA): respect, privacy, sharing, and safety.

The following policies, procedures, and guidelines are provided to help understand what is acceptable use of ICT and can be applied anywhere including by parents in their homes. In making decisions regarding student and staff access to the district's ICT resources, HVPS considers its own educational objectives, goals, and strategic direction. It is important that staff, students, and parents review this AUP and agree in writing to all included administrative regulations and guidelines. Noncompliance may result in suspension of access or termination of privileges and other disciplinary action consistent with HVPS policies. Violations of law may result in criminal prosecution as well as disciplinary action by HVPS

- **General Access Expectations**

In providing access to our ICT resources, HVPS expects use to be ethical, respectful, academically honest and supportive of the District's mission. Instructional staff are expected to blend thoughtful, purposeful use of the ICT throughout their curriculum and provide guidance and modeling for students in proper use. Students are expected to use the ICT in support of classroom activities, district-sponsored extra-curricular activities, and educational research.

ICT resources include all hardware, software, network resources, bandwidth, licenses, communication devices and mediums purchased or leased by HVPS. All ICT resources are considered extensions of the district's physical space, including while attending school-sponsored events that are off campus and access of HVPS ICT resources via remote-access from home or other locations.

HVPS provides content-filtered Internet access to all devices attached to the district's wide area network in compliance with CIPA. The Internet provides students educational opportunities not accessible locally, access to subject-field experts, communication with diverse groups, the ability to publish and locate educational information, and many other benefits. However, because no filtering technology is 100% safe, students may come across information that can be considered harmful, explicit, or illegal. HVPS makes a good faith effort to protect its students from these materials, and works in partnership with our staff and students to improve the system. All system activity is monitored and logged, and parents may request copies of their child's access. Any use of proxies or other devices to circumvent the HVPS content filter is a breach of this agreement and will result in suspension of Internet access except for classroom approved sites. Ultimately parents and guardians of minors are responsible for setting and conveying standards that their children should follow when using media and information sources.

All ICT resources are owned by the District, therefore all users must be aware that they should not have any expectations of personal privacy in the use of these resources. HVPS has the right to monitor, inspect, review, and store at any time without prior notice any and all usage of the ICT including transmitted and received information. HVPS ICT is a limited forum and HVPS may restrict speech for educational reasons. Any Employee who is transferring or leaving a position must leave all work-related files and ICT resources with the District regardless of authorship for their replacements. Vandalism, disruption, or deletion of any ICT resources may result in fees, loss of privileges or disciplinary action in accordance with District procedures.

Students and staff may use approved personal electronic devices (laptops, mobile devices, etc.) on the HVPS wireless Guest network to further the educational mission of the district. The devices may not impose any tangible burden financial or otherwise on HVPS and are provided limited technical support. A signed Bring Your Own Device (BYOD) agreement must be on file with the HVPS IT Department and building administration. Building staff will retain the final authority in deciding when and how the personal electronic devices may be used on school grounds and during the school day. A school may temporarily hold (pending parental or same-day pick up) personal technology resources that are used inappropriately. Members of the public who are granted access shall agree to comply with all District rules, regulations, and policies governing use of the ICT resources. Members of the public may only be granted access to ICT by HVPS administration and the HVPS ICT Department

- **Safety**

Passwords are provided for each user's personal use only and are, therefore, confidential. Users are responsible for all access and activity under their accounts and should promptly change their password and notify an administrator if they feel their account has been compromised. Stealing, sharing, or using another user's password is a direct violation of this AUP. Password reset privileges are logged and unauthorized changes for non-support purposes will result in loss of privileges and/or disciplinary action. Users are expected to follow the guidelines in Appendix A for strong passwords. Users are expected to respect the privacy of others, therefore they shall not obtain copies, modify, or distribute any files, data, or messages that belong to another user without first obtaining permission.

Students and staff should not reveal personal information on any electronic medium, including a home address or personal phone number. Students and staff may not reveal any personal information of another individual on any electronic medium without appropriate permission. Staff that choose to use social media should follow the guidelines set forth in Appendix B. Users will not use the ICT to knowingly insult, bully, post, transmit or distribute false or defamatory information about a person or organization, or to harass another person, or to engage in personal attacks, including prejudicial or discriminatory attacks. If any user encounters dangerous or inappropriate information or messages, they must contact the appropriate administrative authority.

All students will be educated about about appropriate online behavior, including interacting with other individuals on social networking websites and in chat rooms, and cyberbullying awareness and response. Age-appropriate materials will be made available for use across all grade levels. HVPS will provide training, materials, and curriculum regarding online safety issues for administration, staff, and families.

- **Email**

All staff and students in grades (6-12) are provided email accounts through HVPS's Google Apps for Education account. Student email accounts are important forms of communication between teachers and students, and are monitored and archived along with all staff accounts. HVPS follows the Children's Online Privacy Protection Act (COPPA) which limits the ability of commercial companies to collect personal information from children under 13. By default, Google advertising is turned off for Apps for Education users. No personal student information is collected for commercial purposes. This AUP form allows the school to act as an agent for parents in the collection of information within the school context. The school's use of student information is solely for educational purposes. Email accounts are not created for students in Pre-K through 5th grade, unless requested. In the event of such a request, HVPS will notify parents of the request.

HVPS email accounts are for educational use and may not be used for address harvesting, religious or political campaigning, commercial purposes, spamming, or any other use not aligned to the educational mission of HVPS. All email accounts are archived and retained per retention guidelines, barring power outages or intermittent technical failures.

- **Copyright / Plagiarism**

Downloading, duplicating, copying, and distributing software, images, sound files, audio-visual files, and any other copyrighted materials without the specific written permission of the copyright owner is generally prohibited. Distribution of content shall follow Copyright Law and Fair Use Guidelines.

- **Publishing**

During the course of the year, HVPS may publish pictures or stories through various electronic mediums to promote the positive activities, honors, and events of our staff and students. These publications may include likenesses, information, and pictures. Please note, however, that your child's image or likeness may appear in occasional candid photos without any type of name identification and the use of these candid photos of your child is permissible. Students who attend extracurricular activities forfeit their rights to retain authority over the publication of photos taken. All content representing the school district published by ICT users should follow district policies and state/federal laws pertaining to content standards, student records, copyright, and technical standards.

- **Unacceptable Use**

Unacceptable use of ICT resources includes, but is not limited to:

- Sending, storing, or displaying offensive messages or pictures.
- Using obscene language.
- Giving personal information, such as complete name, phone number, or address without proper consent.
- Cyberbullying, hate mail, harassing, insulting or attacking others, discriminatory jokes and remarks.
- Damaging or modifying ICT resources.
- Distributing viruses, malware, bloatware, or illegal software.
- Violating copyright laws.
- Sharing, using, modifying other users logons, passwords, or other personal/confidential information.
- Trespassing in others' folders, work, or files.
- Intentionally wasting limited resources
- Posting information sent or stored online that could endanger others.
- Employing ICT resources for non-academic, personal, commercial, political or religious purposes, financial gain, or fraud.

- Attaching unauthorized equipment to the HVPS network.

- **Terms of Agreement**

HVPS ICT resources are provided on an “as is, as available” basis. Use of the resources is at the user’s own risk, and HVPS will not be responsible for any damages which may occur. Opinions, advice, services, and all other information expressed by the system users, information providers, service providers, or other third-party individuals in the system are those of the providers and not HVPS. HVPS is not responsible for financial burdens or loss incurred from unauthorized use of ICT resources. All users agree to comply and abide by the guidelines set forth in this agreement, and understand that violation of any part could result in loss of privileges, disciplinary action, including suspension or expulsion from school, and/or legal action. HVPS will cooperate fully any law enforcement agency investigations related to illegal activities conducted using HVPS ICT resources.

Hatch Valley Public Schools
Information & Communication Technologies
Student Acceptable Use Policy (AUP) Agreement

Student

- By signing below, I agree that I have read, understand, and will abide by the Hatch Valley Public Schools Acceptable Use Policy for Information & Communication Technologies. I understand that my use of these resources is a privilege and requires proper online etiquette. I also agree to report any misuse of these resources to a HVPS faculty or staff member and that misuse will result in disciplinary action.

Student Name (Print) ____

Student Signature: ____

Date: _________________ Grade: __________________ School:_________________

Parent or Guardian

As the parent or guardian of this student, I have read, understand, and agree to support the Hatch Valley Public Schools Acceptable Use Policy for Information & Communication Technologies. I agree to defend, indemnify and hold harmless HVPS from any and all claims arising out of or related to the use of the Information & Communication Technologies. I further understand that I have the right to withdraw my approval in writing at any time.

Approved

Disapproved

Parent/Guardian Name (Print)

____

Signature of Parent/Guardian:

____

Date: ____

Hatch Valley Public Schools
Information & Communication Technologies
Employee / Public Acceptable Use Policy (AUP) Agreement

User (Employee / Member of Public)

____
(Print User Name)

I have read, understand, and will abide by the Hatch Valley Public Schools Acceptable Use Policy for Information & Communication Technologies (ICT). Should I commit any violation or in any way misuse my access to the HVPS ICT resources, I understand that my access privilege may be revoked and disciplinary action may be taken against me.

____
(User Signature) (Date)

Appendix A
Hatch Valley Public Schools
Strong Password Guidelines

- **Overview**

User passwords are the front line of security for users' personal information and the security of the HVPS network. A weak or easily hacked password can compromise the user's account and potentially the entire computer network. As such, all HVPS authorized account holders that have access to any Information & Communication Technologies resources are responsible for taking the appropriate steps for selecting and securing their passwords. All passwords should be treated as sensitive, confidential information.

- **Password Guidelines**

Strong passwords:

1. Contain both upper and lower case characters (e.g., a-z, A-Z)
2. Have digits and punctuation characters as well as letters (e.g., 0!@#$%^&*()+-|~=\[]:";)
3. Are at least 6 alphanumeric letters long.
4. Are not words in any language, slang, dialect, jargon, etc.
5. Are not based on personal information, names of family, etc.
6. Are changed multiple times through the year

Weak passwords:

1. Contain less than 6 characters
2. Are found in a dictionary
3. Are common usage words (e.g., Names of family, pets, friends, co-workers, characters, etc.)
4. Computer terms and names, commands, sites, companies, hardware, and software.
5. Birthdays and other personal information such as addresses and phone numbers.
6. Word, keyboard, or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
7. Any of the above spelled backwards or followed by a digit (e.g. secret1)

Appendix B
Hatch Valley Public Schools
Staff Social Networking Guidelines

Staff decisions to use online social networking for personal use is at the employee's discretion. HVPS does not affirmatively monitor social networking sites used by employees, if those sites/tools are not being accessed from the district's network; however HVPS may take appropriate action if it becomes aware of, or suspects, conduct or communication on an online social media site that affects the workplace or violates an online code of ethics.

1. Do not accept students as friends on personal social networking sites. Decline any student-initiated friend requests. Professional standards dictate that an adult should never be alone in an isolated space (i.e. one student, one teacher together in a classroom with the door closed after school operating hours). Social networking sites are structured to be closed environments.

Please use district provided tools to communicate with your students, websites, email, forums, Google Groups, etc.

2. Do not initiate friendships with students on social networking sites.

3. Ensure that social networking posts are appropriate for the public. Remember that people classified as friends have the ability to download and share information with others.

4. Do not discuss students, their families, or co workers or publicly criticize school policies or personnel. This includes images obtained through your employment.

5. Weigh whether a posting will put your effectiveness as an employee at risk.

6. Set privacy settings carefully to ensure that you know who has access to the content on your social networking sites.