USD 312 Haven Schools
Acceptable Use Policy (AUP)

This policy sets forth guidelines for acceptable and safe use of USD 312's technology resources, including Internet, network, hardware, and software. The use of these resources is a privilege and not a right. This policy has been adopted by the USD 312 Board of Education, and all users, staff and students, are expected to adhere to these guidelines. Violation of this policy may result in the loss of this privilege, and may result in discipline or criminal charges in accordance with board policy, state and federal law.

Network and Internet

The purpose of providing Internet and access to electronic communication tools for student and staff is to promote resource sharing, innovation, communication, and other 21st Century Skills. Various accounts may be created for teacher-supervised educational experiences.

A content filtering system is utilized to minimize access to inappropriate Internet sites while on the district network, and to comply with the Children's Internet Protection Act (CIPA). Specific categories and levels of filtering will be determined by the District Technology Committee. No filtering system has proven to be 100% accurate, and inappropriate material may occasionally pass through the filter. Inappropriate sites which are not identified by the filter may be submitted to the district technology department for review and appropriate action.

Any communication over the school district network, whether on a district-owned or personal device, should not be considered private and is subject to monitoring. The district reserves the right to access stored data in cases where there is a reasonable suspicion that there has been a violation of this policy.

Acceptable Use

Technology resources are only to be used for purposes which support educational objectives of USD 312. The district requires legal, ethical, responsible and appropriate use of those resources. This applies to:

- District owned technology resources at all times and in all locations.
- Privately owned devices while on district property, at district sponsored events, or while using the district network.

The following acts are prohibited:

1. Attempts to bypass the network or security of content filtering safeguards. This includes using private networks, such as Wi-Fi hotspots, or cellular technologies, such as 3G/4G, for the purpose of circumventing those safeguards.
2. Vandalism, or attempts to damage, interfere or tamper with the proper functioning of district-owned technology resources. This includes, but is not limited to introducing or spreading computer malware.
3. Unauthorized or fraudulent attempts to access information or resources.
4. Sharing personal login credentials for technology resources or accounts.
5. Using technology resources for non-educational purposes. This includes, but not limited to, playing non-teacher approved computer games, and using the network resources to access websites and digital media that do not support class, school, or district goals.
6. Transmission of material in violation of United States or state regulations. This includes, but is not limited to, copyrighted material, threatening or obscene materials, or material protected by trade secret.

7. Transmission of obscene, bullying, profane, lewd, threatening, disrespectful, or gang related language or images. This applies not only to those who directly engage in this conduct, but also to those who have knowledge of and fail to report such conduct to a school administrator.
8. Transmission of images, audio, or language through any digital media, such as websites, blogs, messaging or emails, that is inappropriate by normal classroom standards.
9. Unauthorized distribution of confidential information.
10. The use of technology resources in any locations or in any way that violates another person's reasonable expectation of privacy.
11. The use of technology resources for personal gain, promotion of non-profit or for-profit organizations, commercial activities, product advertisement, religious proselytizing or political lobbying.
12. The use of technology resources in any way that disrupts the normal and safe conduct of school activities.

Security

Any issues with the physical security of technology resources, such as vandalism, theft, or compromised passwords, should be immediately reported to the Director of Technology.

Financial

In the event that the district-owned equipment is used by a student, the student and parent/legal guardian agrees to properly use and care for the equipment, and will assume the risk of loss by theft, destruction, or damage. If the equipment is damaged or returned with any accessories missing or damaged, as determined by the manufacturer or a district technology staff member, the district will charge the student/parent/legal guardian the repair/replacement cost. If the equipment is lost or stolen, the student/parent/legal guardian will be financially responsible for the cost of replacement. In the event that damage occurs, it must be reported immediately to a school administrator. All equipment must be returned when requested. The district reserves the right to seek monetary reimbursement for any and all damages incurred as the result of vandalism.

Disclaimer

Haven USD 312 makes no warranties of any kind, whether expressed or implied, for the service it provides. The district is not responsible for any damages, including loss of data resulting from delays, non-deliveries, mis-deliveries, or service interruptions caused by its own negligence, errors or omissions. The district specifically denies any responsibility for the accuracy of quality of information obtained through its services.

User Agreement

I have read and agree to the terms and conditions of the USD 312 Acceptable Use Policy. I understand that failure to abide by this policy may result in loss or suspension of privileges. I understand that disciplinary action and/or criminal charges may be brought against me for any violation of this policy. I accept the financial obligation outlined in this policy in the event that equipment is checked out to me.

Parents or Legal Guardians who have students under the age of 18 must also sign this form.

_____	_____	_____
Student/Staff Name	Signature	Date
_____	_____	_____
Parent/Legal Guardian Name	Signature	Date