Sheridan AllPrep Academy
Responsible Use Guidelines for Staff

Sheridan AllPrep Academy views the use of electronic resources as central to the delivery of its educational program, and as such maintains the expectation that staff will use electronic resources as an essential part of their learning experiences. It is the policy of Sheridan AllPrep Academy to maintain an environment that promotes ethical and responsible conduct in all electronic resource activities.

Internet and Device Use
The following guidelines are for employee internet use during work. These guidelines include the use of both wired and wireless devices, software, peripheral equipment, computers, tablets, phones, handhelds, files, storage, email, and internet content. Sheridan AllPrep Academy reserves the right to prioritize the use of, and access to, the wired and wireless resources.

Use of school resources must support education and research and be consistent with the mission of the school.

Acceptable Use by School Staff Includes:

- Creating files, projects, videos, web pages, and podcasts using school resources in support of educational research;
- Participating in blogs, wikis, bulletin boards, social media sites, web groups and the creation of podcasts, email and web pages that support educational research;
- Publishing original educational material online, and curriculum related materials and student work. Sources outside the classroom must be cited appropriately.
- Connection of personal electronic devices (wired or wireless) including portable devices with network capabilities to the school internet. Connection of any personal electronic device is subject to all procedures in this document.

Unacceptable Use by School Staff Includes, but is not limited to:

- Using school resources for personal gain, commercial solicitation and compensation of any kind, including using or knowingly allowing another user to use any computer, computer network, computer system, program, or software to devise or execute a scheme to defraud or to obtain money, property, services, or other things of value by false pretenses, promises, or representations.
- Creating liability or cost to the school.
- Downloading, installation, and use of games, audio files, video files or other applications (including software or freeware) without permission or approval of the principal.
- Supporting or opposing ballot measures, candidates, and any other political activity.
- Distributing of unsolicited advertising, hacking, cracking, vandalizing, the introduction and or propagation of computer viruses, works, Trojan horses, time bombs and changes to hardware, software, and monitoring tools, distributing

quantities of information that overwhelm a system (including "chain letters," network games, or broadcasting messages.

- Using school resources to make unauthorized access to other school computers, networks, or information systems, or any other resource via the school resources.
- Attempting to harm, destroy, or interfere with the proper operation of computing hardware, operating systems, applications software of data.
- Invading the privacy of individuals or entities (e.g. use of someone else's account) or misrepresenting other users on the network.
- Cyber bullying, hate mail, defamation, illegal, harassing, inappropriate, or obscene purposes in support of such activities, including discriminatory jokes, remarks, posts, files, or comments on social media sites. This is determined solely by the school.
- Submitting, publishing, displaying, or forwarding any defamatory, inaccurate, racially offensive, abusive, obscene, profane, sexually oriented, or threatening materials or messages.
- Seeking to gain or gaining unauthorized access to information resources, obtaining copies of, or modifying files or other data, or gaining and communicating passwords belonging to other users.
- Posting information sent or stored online that could endanger others.
- Accessing, uploading, downloading, storage, and distribution of obscene, pornographic, or sexually explicit material, as determined at the school's sole discretion.

The school reserves the right, subject to applicable law, to disconnect and check any electronic device of involvement in a violation of school policy. The school also reserves the right to remove any user generated content from sites it owns at any time.

Safety and Security

Staff shall treat their personally identifiable information and that of others in network communications as confidential. Personally identifiable information is defined as complete names, addresses, telephone numbers, and identifiable photos. This includes posting on social media sites, web sites, blogs, podcasts, videos, wikis, and email or as content on any other electronic medium.

The school uses student images and/or student work in school publications, websites, and videos, to promote student achievement and special events. News media may also take photos/videos for education-related storied involving our school. Student names will not be posted directly with images, but may be given in reference to news stories.

Personal Devices

By connecting a mobile device to the Sheridan AllPrep Academy internet and email system, you acknowledge and agree that Sheridan AllPrep Academy reserves the right to enforce any security measures deemed necessary. This includes, but is not limited to:

- Remotely deleting the contents of your mobile device. This may include school and personal contacts, pictures, etc.
- Enforce the use of a password/pin to access the mobile device.
- Restrict the use of applications deemed a security risk.

In addition, you must understand that documents or records, including electronic communications of a public agency, are public records under Oregon state law. Using any personal device or computer for school business can result in a requirement that you submit your personal device for examination or search if a public records request is received concerning information that may be stored on your personal device.

Copyright

Use of the school resources must be in compliance with all copyright law.

Violation of such matters as institutional or third-party copyright, license agreements, or other contracts is prohibited. The unauthorized use of and/or copying of software is illegal and prohibited. The unauthorized installation, storage, or distribution of copyrighted software or material is prohibited.

Downloading, copying, duplicating and distributing software, music, sound files, movies, images or other copyrighted materials without specific written permission of the copyright owner is generally prohibited. The duplication and distribution of materials for educational purposes are permitted when such duplication and distribution fall within the Fair Use Doctrine of the United States Copyright Law (Title 17, USC) and cited appropriately.

All student work is copyrighted. Permission to publish any student work requires permission from parent or guardian.

Security

Passwords are the first level of security for a user account. System logins and accounts are to be used only by the authorized owner of the account, for authorized school purposes. Staff is responsible for all activity on their account and must not share their account password.

No Expectation of Privacy

The school provides technology resources as a tool for education and research in support of the school's mission. All content belongs to the school.

No user should have any expectation of privacy when using the school's resources. The school reserves the right to monitor, intercept, retrieve, and otherwise use and disclose all access, use transmissions, communications and information ever in or passing through school resources, with or without the consent of the user. The school reserves the right to disclose to law enforcement officials or third partied as appropriate.

All files are subject to the public records disclosure laws of the State of Oregon.

Sanctions for Violations

Any activity that violates this policy should be reported to the school administrator. Disciplinary action, if any, shall be consistent with the school's standard policies and procedures. Violations of the User Agreement can constitute cause for revocation of access privileges, suspension of access to resources, termination of employment, and other appropriate legal or criminal action including restitution, if appropriate.

PLEASE REVIEW THESE GUIDELINES CAREFULLY, SIGN, AND RETURN

I hereby agree to comply with all the above stated guidelines. I understand that unacceptable use of the school resources, including equipment, software, internet, and email, is not tolerated and will result in disciplinary action.

_____ _____

Staff Name (printed) Staff Signature

_____

Date