Electronic Information System (Networks)

ACCEPTABLE USE GUIDELINES

Network

1. All use of the system must be in support of education and research and consistent with the mission of the district. The district reserves the right to prioritize use and access to the system.

2. Any use of the system must be in conformity to state and federal law, network provider policies and licenses, and district policy. Use of the network for commercial solicitation is prohibited. Use of the system for charitable purposes must be approved in advance by the administration or designee.

3. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.

4. No use of the system shall serve to disrupt the operation of the system by others; system components including hardware or software shall not be destroyed, modified, or abused in any way.

5. Malicious use of the system to develop programs that harass other users or gain unauthorized access to any computer or computing system and/or damages the components of a computer or computing system is prohibited.

6. Users are responsible for the appropriateness and content of the material they transmit or publish on the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are expressly prohibited.

7. Use of the system to access, store, or distribute obscene or pornographic material and material leading to or promoting violence is expressly prohibited.

8. Subscriptions to mailing lists, bulletin boards, commercial on-line services, and other information services must be pre-approved by the administration or designee.

Security

9. System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users may not share their account number or password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their account.

10. Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users, or misrepresent other users on the system or attempt to gain unauthorized access to the system.

11. Communications may not be encrypted so as to avoid security review.

12. Users should change their passwords regularly and avoid easily guessed passwords.

Personal Security

13. Personal information such as addresses and telephone numbers should remain confidential when communicating on the system. Students should never reveal such information without permission from their teacher and parent or guardian. No user may disclose, use, or disseminate personal identification information regarding minors without authorization.

14. Students should never make appointments to meet other people in person who they have contacted on the system without district and parental permission.

15. Students should notify their teacher or other adult whenever they come across information or messages that are dangerous, inappropriate, or make them feel uncomfortable on the web or when using electronic mail, chat rooms, or other forms of direct communications (i.e. Instant Message services).

16. The unauthorized installation, use, storage, or distribution of copyrighted software or materials on district computers is prohibited by federal law.

Filtering and Monitoring

17. Filtering hardware/software is now in use on all district computers with access to the Internet. This filtering solution will block or filter access to visual depictions that are obscene, child pornography, or harmful to minors. When adults are using the Internet, materials which are obscene and child pornography will still be filtered or blocked.

18. Educational staff will, to the best of their ability, monitor minors' use of the Internet in school, and will take reasonable measures to prevent access by minors to inappropriate material on the Internet and World Wide Web, and restrict their access to materials harmful to minors.

General Use

19. Diligent effort must be made to preserve system resources. For example, users should frequently delete e-mail and unused files.

20. No person shall have access to the system without having received appropriate training. A signed Individual User Release From must be on file with the district. Students under the age of 18 must have the approval of a parent or guardian.

21. Nothing in these regulations is intended to preclude the supervised use of the system while under the direction of a teacher or other approved user acting in conformity with the district policy and procedure.

From time to time, the district will make a determination on whether specific uses of the system are consistent with the regulations shown above. Under prescribed circumstances non-student or staff use may be permitted, provided such individuals demonstrate that their use furthers the purpose and goals of the district. For security and administrative purposes, the district reserves the right for authorized personnel to review system use and file content. The district reserves the right to remove a user account on the system to prevent further unauthorized activity. The district's wide area network provider reserves the right to disconnect the district to prevent further unauthorized activity.

Violations of any of the conditions of use may be cause for disciplinary action.

ELECTRONIC INFORMATION SYSTEM (NETWORKS)
INDIVIDUAL USER ACCESS INFORMED CONSENT

In consideration for the privilege of using the network, and in consideration for having access to the public networks, I hereby release the White Pass School District No. 303 and other intermediary providers, if any, and operators and any institutions with which they are affiliated, from any and all claims and damages of any nature arising from my or my child's use, or inability to use the network including without limitation the type of damages identified with the White Pass School District No. 303 Acceptable Use Guidelines. Further, my child and I agree to abide by the District's Policy and Procedures for Electronic Information Systems, which we have reviewed and understand, and we acknowledge and agree that the White Pass School District No. 303 has the right to review, edit or remove any materials installed, used, stored, or distributed on or through the network or District's system, and we hereby waive the right of privacy which my child or I may otherwise have into such material.

_____	_____
Signature of User	Signature of Parent/Guardian (Required if user is under 18 years of age)
_____	_____
Printed Name of User	Printed Name of Parent/Guardian
_____	_____
Address	Address
_____	_____
City, State, ZIP	City, State, ZIP
__(____)_____	__(____)_____
Phone	Phone
_____	_____
Date Signed	Date Signed

*Students over the age of 18 do not need a parent/guardian's signature.

Desired Password: _____

Passwords **must be at least 7 characters long and contain **uppercase**, **lowercase**, and **numeric** characters. Passwords **cannot contain your name!** Example: Pa55w0rd*

Do not write below this line.

Account: _____ **Date Approved:** _____

Approved By: _____