

Snoqualmie Valley Public Schools
Electronic Information Systems
Internet Safety and Acceptable Use Guidelines

Network Use

All use of the system must be in support of education and research and consistent with the mission of the district. Use of the Network for personal communication shall be at the discretion of the superintendent or designee. District reserves the right to prioritize use and access to the system.

Any use of the system must be in conformity to state and federal law, K-20 Network policies, and district policy. Use of the system for commercial solicitation is prohibited. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures. Use of the computers or network systems for personal profit or gain is also prohibited. The superintendent or designee must approve use of the system for charitable purposes in advance.

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.

Malicious use of the system to develop programs or institute practices that harass other users or gain unauthorized access to any entity on the system and/or damage the components of an entity on the network is prohibited.

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

Use of the system to access, store, or distribute nudity, pornography, violence, crime, drug use, discrimination or other inappropriate material is prohibited.

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

Network Security

System logins or 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. For reasons of systems and personal security, each system account holder must authorize district review of e-mail messages.

Users shall not seek information on, obtain copies of, or modify files, other data, or passwords belonging to other users; misrepresent other users on the system; or attempt to gain unauthorized access to any entity on the K-20 Network.

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

Users should change passwords regularly and avoid easily guessed passwords.

Personal Security

Personal information such as complete names, addresses, telephone numbers and identifiable photos should remain confidential when communicating with an unfamiliar person. 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.

Students should never make appointments to meet people in person whom they have contacted on the system without district and parent permission.

Student and employee users should notify their building principal whenever they come across information or messages they deem dangerous or inappropriate on the web or when using electronic mail, chat rooms, and other forms of direct electronic communications (i.e. Instant Message services).

Copyright

The unauthorized installation, use, storage, or distribution of copyrighted software or materials on district computers is prohibited. All users of the K-20 Network shall comply with current copyright laws.

Filtering and Monitoring

The Snoqualmie Valley School District conforms to the Internet Safety Policy recommendations of the federal Children's Internet Protection Act (CIPA) which includes computer monitoring and the use of an Internet Filtering Solution and which seeks to address the following:

1. access by minors to inappropriate matter on the Internet and World Wide Web;
2. the safety and security of minors when using electronic mail, chat rooms, and other forms of direct electronic communications;
3. unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
4. unauthorized disclosure, use, and dissemination of personal information regarding minors;
5. minors' access to materials harmful to minors

General Use

Diligent effort must be made to conserve system resources. For example, users should frequently delete E-mail and unused files, and users should promptly disconnect videoconferences on completion.

Appropriate training should occur and a signed Individual User Informed Consent Form must be on file with the district before access is granted. Students under the age of 18 must have the approval of a parent or guardian.

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

From time to time, the district will make a determination on whether specific uses of the K-20 Network are consistent with the regulations stated 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 network use and content. The district reserves the right to remove an individual's network access privileges to prevent further unauthorized activity.

Discipline

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

Disciplinary action, if any, for students, staff, and other users shall be consistent with the District's standard policies and practices. Violations may constitute cause for revocation of access privileges, suspension of access to District computers, other school disciplinary action, and/or appropriate legal action. Specific disciplinary measures will be determined on a case-by-case basis.