

**Network Acceptable Use Guidelines/Internet Safety Requirements:**

## A. Network

1. All use of the system must be in support of education and research and consistent with the mission of the district. District staff may use the network for incidental personal use. Such use shall be in accordance with all district policies and guidelines regarding computers, networks, and web pages. Such use shall not result in personal gain or compensation to staff members and shall not incur any cost to the district. The district reserves the right to prioritize uses and access to the system.
2. Any use of the system must be in conformity to applicable state and federal law, K-20 network policies and licenses, and district policy. Use of the system for commercial solicitation of any kind is prohibited.
3. No games, audio files, video files, or other applications may be downloaded or installed by students without permission of the site administrator or designee. The purpose of any downloads must be in support of education and research.
4. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.
5. No use of the system shall serve to disrupt the operation of the system by others, including 'hacking,' introduction of viruses, or other unlawful activities; system components including hardware or software shall not be destroyed, modified, or abused in any way.
6. Malicious use of the system to develop programs that harass other users or gain unauthorized access to any computer or computing system and/or damage the components of a computer or computing system is prohibited.
7. Users are responsible for the appropriateness and content of material they transmit or publish on the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are expressly prohibited. Nor is the system to be used to access or publish information potentially endangering the public, e.g., bomb construction or drug manufacture.
8. Uses of the system to access, store, or distribute obscene or pornographic material is prohibited.
9. Participation in chat rooms, bulletin boards, and other like services must be in support of education and research and approved in advance by the superintendent or designee.
10. All class and school web pages must contain original educational or curriculum related materials, and/or original student work. Staff members are responsible for all materials and content on their web pages. Any source outside the classroom or school must be cited on the web page.
11. Students' personal computers or laptops may not be connected to the district network. Staff members wishing to connect personal laptops to the district network must check with the school Technology Specialist to assure that the appropriate up-to-date virus software is loaded on the laptop, a compatible network card installed, and the laptop is configured properly.

12. Network equipment (switches, routers etc) will be connected and maintained by District Network personnel ***only***. Any unauthorized equipment found connected to the district network will be confiscated.
13. No user may use the system in a way that creates a risk of liability or actual liability or cost to the district.

#### B. Security

1. Issaquah student data is accessed through Skyward, Ed Data Solutions, OSPI, and the Issaquah School District. Confidential student data is used within ISD by district staff for diagnostic and planning purposes only. No student data or confidential files may be left open, unattended, or unsecured. All district employees are bound by state and federal confidentiality laws.
2. System logins or accounts are to be used only by the authorized owner of the account for authorized purposes. Users may not share their accounts or passwords with another person. Account owners are ultimately responsible for all activity under their account.
3. 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 access to any entity on the K-20 Network.
4. Communications may not be encrypted so as to avoid security review.
5. Users should change passwords regularly and avoid easily guessed passwords.
6. *Electronic communications on the networks are not confidential or private.* The district reserves the right to access and monitor network use and messages sent or received over or stored in the system. While the district does not have a practice of monitoring communications, it may do so where appropriate, such as in connection with an investigation of misconduct or for administrative or security purposes. The district reserves the right to disclose any electronic message to law enforcement officials or third parties as appropriate. Users should be aware that even though they have selected and use a personal password, the district may still access their communications.

#### C. Personal Security

1. Personal information such as addresses and telephone numbers should remain confidential when communicating on the system. Users should never reveal such information without permission from the Director of Educational Technology. No user may disclose, use, or disseminate personal identification information regarding minors without authorization of Director of Educational Technology.
2. No student pictures, names, art work, writing, audio files, or video files may be published on the class, school, or district web site unless a signed Individual User Access Informed consent and Release Form is on file with the district.
3. Student should never make appointments to meet people in person that they have contact on the system without district and parent permission.
4. Users should notify an appropriate person whenever they come across information or messages that are dangerous or inappropriate, while on the web, or when using electronic mail, chat rooms, and other forms of direct electronic communications.

Students should notify a teacher of such matters and teachers and staff should bring such matters to the attention of the Director of Educational Technology.

D. Copyright

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

E. Filtering and Monitoring

1. Filtering software is used to block or filter access to visual depictions that are obscene, child pornography, or harmful to minors. All materials which are obscene and child pornography must be filtered or blocked.
2. 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.

F. General Use

1. Diligent effort must be made to conserve system resources. For example, users should frequently remove from the system e-mail and unused files, and users should promptly disconnect videoconferences on completion.
2. No person shall have access to the K-20 Network without having received appropriate training. A signed individual User Access Informed Consent and Release Form must be on file with the district. Students under the age of 18 must have the approval of a parent or guardian.
3. 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 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 that such individuals demonstrate that their use furthers the purpose and goals of the district. The district reserves the right to remove an individual's network access privileges to prevent further unauthorized activity. The district's wide-area network provider (Washington K-20) reserves the right to disconnect the district to prevent further unauthorized activity.

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

Revised October 24, 2001  
Revised October 23, 2002  
Revised September 17, 2003  
Revised March 30, 2004  
Revised September 1, 2004