NETWORK ACCEPTABLE USE GUIDELINES/INTERNET SAFETY POLICY

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 policy and licenses, and district policy. Use of the system for commercial solicitation is prohibited. Use of the system for charitable purposes must be approved in advance by the Superintendent 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 computer system and/or damage the components of a computer or computing systems is prohibited.

6. Users are responsible for the content of materials they transmit or publish on the system.

7. Use of the system to access, store or distribute material that is obscene, pornographic or considered harmful to minors is prohibited.

8. Software installation must be completed by a district staff member or other approved individual. All installed software **must** be properly licensed. Students are prohibited from installing software on any district computer unless they have prior approval from the Information Systems Department. Additionally, downloading and/or storing executable files (programs) in student home folders is prohibited.

9. Any violation of the requirements of this policy, procedure, or any other student or employee conduct rules applicable to the use in question may subject the user to student disciplinary action or personnel disciplinary action up to and including suspension or expulsion of students or termination of employment.

10. The system administrators of the district network reserve the right to remove users access to the system if at any time it is determined that the user has violated one or more standards contained in Bainbridge Island School District Procedure 2315: Network Acceptable Use

Guidelines/Internet Safety Policy. A user's right to access the system shall not be denied or removed without just cause.

11. No person shall have access to the system without having received appropriate training/orientation, including the review of the Network Acceptable Use Guidelines/Internet Safety Policy and Procedure. Parents of all students will be provided with access to the Network Acceptable Use Guidelines/Internet Safety Policy and Procedure. In addition, parents of students under the age of 18 will be provided with the opportunity to deny or limit network access for their child(ren).

SECURITY

1. System accounts are to be used only by the authorized owner of the account for the authorized purpose. Users are expected to maintain appropriate password confidentiality. Account owners are ultimately responsible for all activity under their account.

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

3. The district has the right to review or remove materials installed, used, stored, or distributed on or through the network.

INTERNET SAFETY

1. The District has implemented a filtering solution designed to comply with CIPA (Children's Internet Protection Act) guidelines.

    A. Filtered Content – Consistent with CIPA guidelines, the District filters Internet content that is obscene, child pornography, or harmful to minors. "Harmful to minors" is defined in CIPA as any picture, image, graphic image file, or other depiction that:

        a. taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion;

        b. depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, an actual or simulated sexual act or sexual contact, actual or simulated normal or perverted sexual acts, or a lewd exhibition of the genitals; and

        c. taken as a whole, lacks serious literary, artistic, political, or scientific value as to minors.

B. Cyber Patrol has been selected as the content filter for the District. Cyber Patrol provides a broad spectrum of categories to select from when filtering Internet content and is very flexible in it's implementation. The following categories are currently being filtered; full nudity, partial nudity, sexual acts, gross depictions, and militant/extremist.

C. All staff and students are required to login to the content filter using a login ID and password prior to accessing the Internet. This provides additional security and helps to increase the accountability of individuals as they access the Internet.

D. Process for review of filtered content – In the likely event that content needs to be added to or removed from the list of filtered Internet sites, the District's Instructional Materials Review Committee will be charged with the responsibility to review any additions or deletions and make appropriate recommendations to the Superintendent and Board of Directors. The Instructional Materials Review Committee will meet on an as needed basis to consider requested changes to the filtered content list.

2. The district will provide appropriate adult supervision of Internet use. The first line of defense in controlling access by minors to inappropriate material on the Internet is deliberate and consistent monitoring of student access to district computers. With this in mind the following guidelines apply to students as they access the Internet.

   A. Student use of electronic mail is prohibited. Exception to this shall be based upon prior approval of a staff member, and such use will be for educational purposes only.

   B. The use of chat rooms, instant messaging services, and other forms of direct electronic communication is prohibited, unless use is under the direct supervision of a staff member or approved adult/parent volunteer, and use is directly related to an educational activity.

3. The district will provide training for staff and students focusing on the development of the skills necessary to make safe, lawful and appropriate use of the Internet in an educational environment.

COPYRIGHT

The installation of copyrighted software or materials on district computers must comply with school district Policy 2312: Copyright Compliance.

PERSONAL SECURITY AND GENERAL USE GUIDELINES

Consistent with the goals and objectives referenced in the Bainbridge Island School District Essential Learnings in Technology and their associated benchmarks, the following priority guidelines are essential to the safe and efficient use of our information network system.

- Personal information, such as address and telephone numbers, should remain confidential when communicating on the system. Students should never reveal such information without permission of their teacher and parent/guardian. Additionally, photos of students containing the identity of said students, shall not be posted on any page of the district web site, without the express written consent of a parent/guardian.

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

- Students should notify their teacher or other adult whenever they come across information or messages that are in their judgment, dangerous or inappropriate.

- Diligent effort must be made to conserve system resources. For example, users should frequently delete e-mail and unused files. The storage of large quantities of video and audio files (avi's, mp3's, mpg's etc…) is strongly discouraged. Users found to have excessive amounts of these types of files will be asked to delete them. If files are not deleted in a timely manner, they will be deleted by the Information Systems Department.