

**INSTRUCTION**ELECTRONIC INFORMATION SYSTEM (K-12 NETWORK)

## K-12 Network Acceptable Use Guidelines/Internet Safety Requirements

Network Use

1. All use of the system must be in support of educational and research and consistent with the mission of the district. Employees must not use the Network for non-instructional purposes during instructional times. 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, K-12 Network policies and district policy. Use of the system for commercial solicitation is prohibited.
3. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures. Any information recorded or accessed on the Network may be disclosable under state law.
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 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.
6. 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. Students, employees and others are responsible for appropriate behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are public in nature, since the Network is owned by the District. General school rules for behavior and communications apply.
7. Use of the system to access, store, or distribute obscene, pornographic or inappropriate material is prohibited.
8. 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 their designee.

Security

1. 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.
2. 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 Network.
3. Communications may not be encrypted so as to avoid security review.

4. Users should change passwords regularly and avoid easily guessed passwords. Users must only use only their own personal password.
5. Users, including students, are required to notify their teacher, adult or District representative whenever they come across information or messages that are dangerous, inappropriate or make them feel uncomfortable.

#### Personal Security

1. Personal information such as complete names, address, telephone numbers and identifiable photos 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 identifiable information regarding minors without authorization.
2. Students should never make appointments to meet people in person whom they have contacted on the system without district and parent permission.
3. Students should notify their teacher or other adult whenever they come across information or messages they deem dangerous or inappropriate on the web or when using electronic mail, chat rooms, or 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 Network shall comply with current copyright laws.

#### Privately Owned Software

Software owned by individuals in the District may be brought into the District under the following conditions:

- a. The user can prove ownership.
- b. The user adheres to the licensing agreement for that software.
- c. The user has registered the software with the Software Company.
- d. The software is clearly for educational activities.
- e. The software is compatible with the LAN and WAN.

#### Filter and Monitoring

1. The Network currently has filters to block or filter out visual depictions that are obscene, pornographic, harmful or harmful to minors. However, every user has the responsibility to prevent and/or immediately report any such occurrences to the Information Technology Department. Failure to do so will result in the loss of access privileges.
2. Education staff will monitor students' use of the Internet in school, and will take reasonable measures to prevent access by minors to inappropriate materials on the Internet and World Wide Web, and restrict their access to materials harmful to minors.

General Use

1. 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.
2. No person shall have access to the Network without having received appropriate training and a signed Individual User Release form must be on file with the district. In addition, 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 network while under the direction of a teacher or other 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 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, with or without notice, to prevent further unauthorized activity. Violations of any of the conditions of use may be cause for disciplinary action.

Adopted: November 8, 1995  
Amended: August 22, 2001