

ELECTRONIC INFORMATION SYSTEMS (NETWORKS)

Acceptable Network and Internet Use Procedures and Guidelines

I. Network Use

- A. All use of the systems must be in support of education and research or District-approved extra curricular activities and consistent with the mission of the District. The District reserves the right to prioritize use and access to the system.
- B. Any use of the system must be in conformity to state and federal law, network provider policies and District policy. Use of the system for commercial solicitation is prohibited.
- C. The system constitutes public facilities and may not be used to support or oppose political candidates or ballot measures.
- D. 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.
- E. 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.
- F. Users are responsible for the appropriateness and content of material they store, transmit, or publish on the system. Hate mail, harassment, discriminatory remarks, or other antisocial behaviors are expressly prohibited.
- G. Use of the system to access, store or distribute obscene or pornographic material is prohibited.

II. Security

- A. 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 password with another person or leave an open file or session unattended or unsupervised. Account owners are ultimately responsible for all activity under their accounts.
- B. 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 any entity on the system.
- C. Communications may not be encrypted so as to avoid security review.
- D. Users should change passwords regularly and avoid easily guessed passwords.

III. Personal Security

- A. Personal information such as complete names, addresses and 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 parents or guardian. No user may disclose, use, or disseminate personal identification information regarding minors without authorization.

B. Students are prohibited from making appointments to meet people in person whom they have contacted on the system without parental permission.

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

IV. Copyright

A. 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.

V. Filtering and Monitoring

A. Filtering services are now in use on all computers with access to the Internet. This 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 must still be filtered or blocked.

B. 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.

VI. General Use

A. 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.

B. No person shall have access to the system without having received appropriate training. A signed Individual User Access Informed Consent Form must be on file with the District. Students under the age of 18 must have the approval of a parent or guardian.

C. 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.

D. From time to time, the District will make a determination on whether specific uses of the system 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 system use and file content including, without limitation, the content of any electronic mail.

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.

Violation of any of the conditions of use is cause for disciplinary action.