ELECTRONIC INFORMATION SYSTEMS (NETWORKS)

Acceptable Use Procedures and Guidelines

I. Network

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 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.

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 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.

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 materials is prohibited.

II. Security

A. System 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, or 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 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 addresses and telephone numbers should remain confidential when communicating on the system. Students should never reveal such information without permission from their parents.

B. Students will never make 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 that are dangerous, inappropriate or make them feel uncomfortable.

IV. Copyright

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

V. General Use

A. Diligent effort must be made to conserve system resources. For example, users should frequently delete E-mail and unused files.

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 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.

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