Student Access to Networked Information Resources

PROGRAM DEVELOPMENT

Staff will provide developmentally appropriate guidance to students as they make use of telecommunications and electronic information resources to conduct research and other studies related to the District curriculum. All students will be informed by staff of their rights and responsibilities as users of the District network prior to gaining access to that network, either as an individual user or as a member of a class or a group.

As much as possible, access to District information resources will be designed in ways that point students to those which have been reviewed and evaluated prior to use. While students may be able to move beyond those resources to others which have not been evaluated by staff, they shall be provided with guidelines and lists of resources particularly suited to the learning objectives. Students may pursue electronic research independent of staff supervision only if they have been granted parental permission and have submitted all required forms. Permission is not transferable and may not be shared.

Except in cases involving students who are at least eighteen (18) years of age and have no legal guardian, parents/guardians may request that the school/District:

- Provide access so that the parent may examine the contents of their child(ren)'s email files;
- Terminate their child(ren)’s individual email account and/or Internet access; and
- Provide alternative activities for their child(ren) that do not require Internet access.

Parents/guardians wishing to challenge information accessed via the District’s technology resources should refer to Policy 08.2322/Review of Instructional Materials and any related procedures.

INTERNET RULES

Students are responsible for good behavior on school computer networks just as they are in a classroom or a school hallway. Communications on the network are often public in nature. General school rules for behavior and communication apply.

The network is provided for students to conduct research and to communicate with others. Independent access to network services is provided to students who agree to act in a considerate and responsible manner. Parental permission is required for minors. Access is a privilege, not a right. Access entails responsibility.

Individual users of the District computer networks are responsible for their behavior and communications over those networks. It is presumed that users will comply with District standards and will honor the agreements they have signed.

Network storage areas may be treated similar to school lockers. The Superintendent/designee may review files and communications to maintain system integrity and insure that users are using the system responsibly. Users should not expect that files stored on District servers or through District provided or sponsored technology services, will always be private.

Student Access to Networked Information Resources

INTERNET RULES (CONTINUED)

During school, teachers will guide younger students toward appropriate materials. Outside of school, families bear responsibility for such guidance as they must also exercise with information sources such as television, telephones, movies, radio and other potentially offensive media.

The following misbehaviors are not permitted:

1. Violating State and Federal legal requirements addressing student and employee rights to privacy, including unauthorized disclosure, use and dissemination of personal information.
2. Sending or displaying offensive messages or pictures, including those that involve:
   - Profanity or obscenity; or
   - Harassing or intimidating communications.
3. Organizing political campaigns.
4. Engaging in practices that threaten the network. (e.g. loading files that may introduce a virus)
5. Violating copyright laws, including illegal copying of commercial software and/or other protected material.
6. Using other's password.
7. Trespassing in other's folders, documents, or files.
8. Intentionally wasting limited resources, including downloading of freeware or shareware programs.
9. Employing the network for commercial purposes.
10. Violating regulations prescribed by the network provider.
11. Conducting union business.
12. Preparing or assembling materials for religious institutions.

Sanctions

1. Violations may result in a loss of access.
2. Additional disciplinary action may be determined at the building level in line with existing practice regarding inappropriate language or behavior.

   When applicable, law enforcement agencies may be involved.