Jerome Joint School District No. 261

PERSONNEL **5330P**

ACCEPTABLE USE POLICY
STUDENT ACCESS TO NETWORKED INFORMATION RESOURCES

ACCEPTABLE USE POLICY (Amendment)

February 19, 2002

Responsible use

All users are expected to use computing resources in a responsible and efficient manner consistent with the instructional, research and administrative goals of the school district. Users are expected to refrain from engaging in deliberate wasteful practices such as sending chain letters through electronic mail, printing unnecessary listings, printing multiple copies of files, performing unnecessary file downloads, or unnecessarily using workstations for long periods of time when others are waiting for these resources. In addition, the playing of games or using computer networks for purely recreational purposes during the instructional day, may compromise network performance and represent irresponsible use of equipment and resources.

The Jerome School District prefers not to act as a disciplinary agency or to engage in policing activities. However, in cases of unauthorized or irresponsible behavior, the Jerome School District reserves the right to take remedial action, commencing with an investigation of the possible abuse.

Overview

The Board recognizes that as telecommunications and other new technologies shift the ways that information may be accessed, communicated and transferred by members of the society, those changes may also alter instruction and student learning. The Board generally supports access by students to rich information resources along with the development by staff of appropriate skills to analyze and evaluate such resources.

Telecommunications, electronic information sources and networked services significantly alter the information landscape for schools by opening classrooms to a broader array of resources. In the past, instructional and library media materials could usually be screened – prior to use – by committees of educators and community members intent on subjecting all such materials to reasonable selection criteria. The Board recognizes that all such materials be consistent with district-adopted guides, supporting and enriching the curriculum while taking into account the varied instructional needs, learning styles, abilities and developmental levels of the students. Telecommunications, because they may lead to any publicly available fileserver in the world, will open classrooms to electronic information resources which have not been screened by educators for use by students of various ages. The Jerome School District #261 will make every attempt possible to filter and prevent offensive material from being accessed by all computer users.

Electronic information research skills are now fundamental to preparation of citizens and future employees during an Age of Information. The Board expects that staff will blend thoughtful use of such information throughout the curriculum and that the staff will provide guidance and instruction to students in the appropriate use of such resources.

Guidelines

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 communications apply. The network is provided for students to conduct research and communicate with others. Access to network services will be provided to students who agree to act in a considerate and responsible manner.

Network storage areas may be treated like school lockers. Network administrators 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 will always be private.

Access to telecommunications will enable students to explore thousands of libraries, databases, and bulletin boards while exchanging messages with people throughout the world. The Board believes that the benefits to students from access in the form of information resources and opportunities for collaboration exceed the disadvantages. But ultimately, parents and guardians of minors are responsible for setting and conveying the standards that their children should follow when using media and information sources.

The following are not permitted:

- Sending or displaying offensive messages or pictures
- Using obscene language
- Harassing, insulting or attacking others
- Damaging computers, computer systems or computer networks
- Violating copyright laws
- Using others' passwords
- Trespassing in others' folders, work or files
- Intentionally wasting limited resources
- Employing the network for commercial purposes

Sanctions

Any user violating these provisions, applicable state and federal laws or posted classroom and district rules is subject to loss of network privileges and any other District Disciplinary options, including criminal prosecution. School and district administrators will make the final determination as to what constitutes unacceptable use and their decision is final.

General Classroom Guidelines

1) **Acceptable Use**
    a. Must be in support of education and research consistent with district policy
    b. Must be consistent with the rules appropriate to any network being used/accessed
    c. Unauthorized use of copyrighted material is prohibited
    d. Threatening or obscene material is prohibited
    e. Distribution of material protected by trade secret is prohibited
    f. Use for commercial activities is not acceptable
    g. Product advertisement or political lobbying is prohibited

2) **Privileges**
    a. Access to the Internet is not a right, but a privilege
    b. Unacceptable usage will result in cancellation of account
    c. Training will be provided for each individual applying for an account

3) **Netiquette**
    a. Be polite
    b. Do not use vulgar or obscene language

c. Use caution when revealing your address or phone number (or those of others)
d. Electronic mail is not guaranteed to be private
e. Do not intentionally disrupt the network or other users
f. Abide by generally accepted rules of network etiquette

4) Security

a. If you identify a security problem, notify a system administrator immediately
b. Do not show or identify a security problem to others
c. Do not reveal your account password or allow another person to use your account
d. Do not use another individual's account
e. Attempts to log on as another user will result in cancellation of privileges
f. Any user identified as a security risk or having a history of problems with other computer systems may be denied access
g. User must notify the district system administrator of any change in account information
h. User may be occasionally required to update registration, password and account information in order to continue Internet access

5) Vandalism/Harassment

a. Vandalism and/or harassment will result in the cancellation of the offending user's account
b. Vandalism is defined as any malicious attempt to harm or destroy data or another user, the Internet or other networks. This includes, but is not limited to, creating and/or uploading computer viruses
c. Harassment is defined as the persistent annoyance of another user or the interference in another user's work. This includes, but is not limited to, the sending of unwanted mail