SHALER AREA SCHOOL DISTRICT

POLICY 244

SECTION: PUPILS
TITLE: ACCEPTABLE USE OF INTERNET
ADOPTED: May 20, 1998
REVISED: April 21, 1999

244. ACCEPTABLE USE OF INTERNET

1. Purpose

The Board supports the use of the Internet and other computer networks in the district's instructional program in order to facilitate learning and teaching through interpersonal communications, access to information, research and collaboration.

The use of network facilities shall be consistent with the curriculum adopted by the school district as well as the varied instructional needs, learning styles, abilities, and developmental levels of students.

2. Authority

The electronic information available to students and staff does not imply endorsement of the content by the school district, nor does the district guarantee the accuracy of the information received on the Internet. The district shall not be responsible for any information that may be lost, damaged, or unavailable when using the network or for any information that is retrieved via the Internet.

The school district shall not be responsible for any unauthorized changes or fees resulting from access to the Internet.

The district reserves the right to log network use and to monitor fileserver space utilization by district users, while respecting the privacy rights of both district users and outside users.

As a condition for using the district's e-mail/network, employees, students, and students' parents shall sign a written consent statement which allows authorized district system support personnel to monitor e-mail/network accounts.

The Board establishes that use of the Internet is a privilege, not a right;

inappropriate, unauthorized and illegal use will result in the cancellation of those privileges and appropriate disciplinary action.

3. Responsibility

The district shall make every effort to ensure that this educational resource is used responsibly by students and staff.

Administrators, teachers, and staff have a professional responsibility to work together to help students develop the intellectual skills necessary to discriminate among information sources, to identify information appropriate to their age and developmental levels, and to evaluate and use the information to meet their educational goals.

Students and staff have the responsibility to respect and protect the rights of every other user in the district and on the Internet.

The building administrator shall have the authority to determine what is inappropriate use, and his/her decision is final.

4. Guidelines

Network accounts will be used only by the authorized owner of the account for its authorized purpose. Al communications and information accessible via the network should be assumed to be private property and shall not be disclosed. Network users shall respect the privacy of other users on the system.

<u>Prohibitions</u>

Students and staff are expected to act in a responsible, ethical, and legal manner in accordance with district policy, accepted rules of network etiquette, and federal and state law. Specifically, the following uses are prohibited:

1. Use of network to facilitate illegal activity.

2. Use of the network for commercial or for profit purposes.

3. Use of the network for non-work or non-school related work.

4. Use of the network for product advertisement or political

lobbying.

5. Unauthorized **transmission** of student records over the Internet.

6. Use of the network for hate mail, discriminatory remarks, and offensive or inflammatory communication.

7. Unauthorized or illegal installation, distribution, reproduction, or use of copyrighted materials.

8. Use of the network to access obscene or pornographic material.

9. Use of inappropriate language or profanity on the network.

10. Use of the network to transmit material likely to be offensive or objectionable to recipients.

11. Use of the network to intentionally obtain or modify files, passwords, and data belonging to other users.

12. Impersonation of another user, anonymity, and pseudonyms.

13. Use of network facilities for fraudulent copying, communications, or modification of materials in violation of copyright laws.

14. Loading or use of unauthorized games, programs, files, or other electronic media.

15. Use of the network to disrupt the work of other users.

16. Destruction modification, or abuse of network hardware and software.

17. Quoting personal communications in a public forum without the original author's prior consent..

18. The Superintendent, or the Superintendent's designee, is directed to develop any further guidelines necessary to carry out the intentions of this policy.

Security

System security is protected through the use of passwords. Failure to adequately protect or update passwords could result in unauthorized access to personal or district files. To protect the integrity of the system, the following guidelines shall be followed:

1. Employees and students shall not reveal their passwords to another individual
, except to approved system support personnel.

2. Users are not to use a computer that has been logged in under another student's or teacher's name.

3. Any user identified as a security risk or having a history of problems with other computer systems may be denied access to the network.

Safety

To the greatest extent possible, users of the network will be protected from harassment or unwanted or unsolicited communication. Any network user who receives threatening or unwelcome communications shall

immediately bring them to the attention of a teacher or administrator.

Network users shall not reveal personal addresses or telephone numbers to other users on the network.

Consequences for Inappropriate Use

The network user shall be responsible for damages to the equipment, systems, and software resulting from deliberate or willful acts.

Illegal use of the network; intentional deletion or damage to files of data belonging to others; copyright violations or theft of services will be reported to the appropriate legal authorities for possible prosecution.

General rules for behavior and communications apply when using the Internet, in addition to the stipulations of this policy. Loss of access and other disciplinary actions
, as outlined in Policy 218, shall be consequences for inappropriate use.

Vandalism will result in cancellation of access privileges. **Vandalism** is defined as any malicious attempt to harm or destroy data of another user, Internet or other networks. This includes but is not limited to the uploading or creation of computer viruses.

Copyright

The illegal use of copyrighted software by students and staff is prohibited. Any data uploaded to or downloaded from the network shall be subject to "fair use" guidelines.

P.L. 94-553
Sec. 107