ACCEPTABLE USE POLICY FOR TECHNOLOGY
EAGLE PASS ISD EMPLOYEES

I agree to follow the regulations listed below while using the computers, the network and its access to the Internet, and all other technology belonging to the Eagle Pass Schools.

1. I will respect and use with care all the technological resources that I choose to utilize.

2. I will keep my account password private, and I will log off the network after I have personally logged in. I understand that all activity using my personal Internet account is my responsibility.

3. I will at all times use technology in a moral and ethical manner and observe network etiquette.

4. I understand that computer games are not permitted to be played without the expressed permission of the immediate supervisor.

5. Software (i.e., licensed, freeware, shareware) brought from home may not be inserted into the computer without the expressed written permission of the immediate supervisor.

6. Faculty/staff will not remove technology equipment without proper consent of an administrator.

7. Students in computer labs shall be supervised at all times.

8. Faculty/Staff are responsible for all technology equipment assigned to them.

9. * I understand that the contents of the Internet will be filtered by the District, but will not assure 100 percent removal of all obscenity/pornography including graphics and bad language.

10. I understand that using technology equipment is a privilege, not a right, and the privilege may be revoked at any time for unacceptable conduct. Unacceptable conduct includes the following: Examples (not a comprehensive list) of policy violations include:

    a. Accessing, or attempting to access, another individual's data or information without proper authorization (e.g., using another ID and password to look at their personal information.)

    b. Obtaining, possessing, using, or attempting to use someone else's password regardless of how the password was obtained (e.g., password sharing)

    c. Tapping phone or network lines (e.g., running network snifters without authorization)

d. Making more copies of licensed software than the license allows (i.e., software piracy)

e. Sending a crippling number of files across the network (e.g., e-mail "bombing")

f. Releasing a virus, worm or other program that damages or otherwise harms a system or network preventing others from accessing services (e.g., taking over a chat channel and kicking other users off)

g. Unauthorized use of school district resources (e.g., using someone else's Remote dial-in access or borrowing their ID and password to access the computer systems)

h. Sending forged messages under some else's ID (e.g., sending hoax messages, even if intended to be a joke)

i. Using school district resources for unauthorized purposes (e.g., using personal computer connected to the campus network to set up web servers for illegal, commercial or profit-making purposes)

j. Unauthorized access to data or files even if they are not securely protected (e.g., breaking into a system by taking advantage of security holes)

Network administration, along with local school administration, will determine disciplinary action taken for infractions involving malicious intent or legalities. More serious consequences may result in information being turned over to the proper authorizes.

EMPLOYEE NO.:	CAMPUS:
I understand, that certified staff might periodically monitor activity on my account. I also understand that failure to follow any of the above rules may result in the loss of access to any technology and the removal of my account from the computer network.	
NAME (PRINT):	TITLE:
SIGNATURE:	DATE:

Technology Use Only	
E-Mail Account Created By:	
Employee No.	Date: