Employee Appropriate Use Policy

Please read the following carefully. Violations of the district **Internet Safety Policy** may cause an employee's access privileges to be revoked, School Board disciplinary action and/or appropriate legal action may be taken, up to and including employment termination. **Additional items that employees need to be aware of:**

1. Staff must be aware that students have access to the Internet from all of the school systems' computers. Teachers must use good judgment and closely supervise their students' use of the Internet. The School System uses filtering software to help prevent student access to inappropriate web sites. However, it is impossible to block access to all objectionable material. If a student decides to behave in an irresponsible manner, he/she may be able to access sites that contain materials that are inappropriate for children or are not commensurate with community standards of decency. Students should not be permitted to access sites unrelated to their assignment and should not be allowed to access game or other sites that could infect the computer with "Spyware".

2. Any individual who is issued a password is required to keep it private and is not permitted to share it with anyone for any reason.

3. Never allow students to log in with a staff member's user name and password. With that information they could log in under the teacher name and look at private documents including email and grades.

4. Be careful when entering your user name and password or changing your password. Do not allow students to look over your shoulder and have access to this information.

5. Never allow a student to use a computer unless they are logged on under their own name (K-2 students may use a generic "classroom account" created by the school ITS).

6. Enforce the Internet Safety Policy while supervising students. It is the employee's responsibility to notify the administration of any violation of the Acceptable Use Policy.

7. Do not allow students to go to computer labs unsupervised.

8. Treat student user names and passwords with confidentiality. Do not post a list of user names and passwords where all students can see them.

9. Users are responsible for the appropriate storage and backup of their data.

10. The system requires employees to change passwords periodically. Some examples of passwords not to use: names of pets, birth date, children's names, street address, school mascots, favorite car, sports team, actor or movie. Make sure any written password

information is stored in a secure location. Do not leave passwords lying on your desk or in an unlocked drawer.

12. Email accounts are provided to employees for professional purposes. Email accounts should not be used for personal gain or personal business activities; broadcasting of unsolicited messages is prohibited. Examples of such broadcasts include chain letters, mail bombs, virus hoaxes, Spam mail (spreading email or postings without good purpose), and executable files. These types of email often contain viruses and can cause excessive network traffic or computing load. All employees must request permission from the building administrator before sending any messages to an entire school staff.

13. Employees must abide by the **Mark Armijo Academy** Web Site Posting guidelines when posting any materials to the web.

14. Employees are not permitted to connect or install any computer hardware, components, or software, which are not school system property to or in the district's technology resources without prior approval of the district technology supervisory personnel.

15. Employees and staff, maintaining or posting material to a Web site or blog that threatens a likelihood of substantial disruption in school, including harming or interfering with the rights of other students to participate fully in school or extracurricular activities is a violation of the Internet Safety Policy.