Computer Anti-Virus Policy

Southwest Area Technology Team Collaborative Draft Policy

1. Purpose

This policy establishes standards and best practices that must be met when any computer or computing device, both wired and wireless, is connected to <District Name> networks to prevent obtaining and spreading computer viruses. These are basic steps that all users must take to ensure that <District Name> computers and networks remain stable and available at all times.

2. Scope

This policy covers all users of computers running any sort of user installable and configurable operating systems (Windows, Mac OS, Linux, etc.) that are used in the District or are connected to the District network either through a wired Ethernet connection or by wireless networking.

3. Policy

3.1 Expectations

3.1.1 Users are expected to use district installed and approved software applications.

3.1.2 Users are not authorized to install unlicensed software on computers. If a user requires special or non-standard software to be installed on computers for District use, it must be cleared by District Technology administration. The user will be responsible for supplying licenses, media, and any documentation. License information is a requirement of the District Auditors.

3.1.3 Users are ultimately responsible for their own data. Users must back up critical data and system configurations on a regular basis and store the data in a safe place.

3.1.4 Users must run the District standard, supported anti-virus software that is available from the District Technology Coordinator or his designees. Users must run the current version and download and install anti-virus software updates as they become available.

3.2 Best Practices

3.2.1 Users must never open any files or macros attached to an email from an unknown, suspicious or untrustworthy source. Users shall delete these attachments immediately, then "double delete" them by emptying the Trash.

3.2.2 Users must delete spam, chain, and other junk email without forwarding, in accordance with the Districts Acceptable Use Policy.

3.2.3 Users shall never download files from unknown or suspicious sources.

3.2.4 Users shall avoid direct disk sharing with read/write access unless there is absolutely a specific District requirement to do so.

3.2.5 Users shall always scan a floppy diskette or any portable storage device from an unknown source for viruses before using it.

3.2.6 New viruses are discovered almost every day. Users shall periodically check the Anti-Virus for updates and download and install any available updates.

3.2.7 Users shall always use the current and up to date version of any software application on school-provided computers. The District will not attempt to make old or outdated software work with newer installed operating systems.

3.3 Results of Non-Compliance

3.3.1 Any non-approved software installations will not be supported.

3.3.2 Any machine that is found to have software installed that has not been approved by the district or does not have a current and active license will be reformatted and all data may be wiped clean.

3.3.3 Any machine that has been infected by a virus that can not be removed from a User's computer will be formatted and wiped clean of all data. The District will reinstall the appropriate system operating software and District approved software only. Any user data on the machine may/will be lost.