

Provo City School District Technology Security Policy

Software Installation Procedure

1. Overview

Allowing employees to install software on company computing devices opens the organization up to unnecessary exposure. Conflicting file versions, older versions of software, or pirated software can prevent programs from running. These and other issues can introduce malware from infected installation software and expose unlicensed software that would be discovered during an audit. Programs, which can be used to hack the organization's network, are also examples of the problems that can be introduced when employees install software on company equipment.

2. Purpose

The purpose of this procedure is to outline the requirements around installation software on PCSD computing devices. Its purpose is to minimize the risk of loss of program functionality, the exposure of sensitive information contained within PCSD's network, the risk of introducing malware, and the legal exposure of running unlicensed software.

3. Scope

This procedure applies to all PCSD employees, with a District owned mobile device. This procedure covers all computers, servers, tablets, personal smart phones, and other computing devices operating within the PCSD network.

4. Procedure

- Employees that handle sensitive information may not install any software that is not District approved. All other Employees may install personal purchased software on PCSD's computing devices operated within the district network with the understanding that it will not be supported by the Help Desk staff in any way. You must contact the manufacturer for assistance. Be sure to check the system requirements on the packaging prior to purchase and installation.
- Copies of "borrowed" software are prohibited. One (1) license equals one (1) installation.
- District Supported Software must be selected from an approved software list, maintained by the Information Technology department. If a specific program is not listed, you may request the purchase through your school's purchasing protocols, keeping in mind that there will be no district support.
- The purchaser of the software will obtain and track the licenses of district-supported software only, test new software for conflict and compatibility, and perform the installation.
- The user should not uninstall District software, upon termination all District owned software shall be removed from the device.
- All employees who choose to connect a personal device on the district network must abide by the same procedure as pertained to district owned devices. The OS software is the

Provo City School District Technology Security Policy

responsibility of each user. All computers must have antivirus software installed prior to connection to the district network. If antivirus software is removed the user will lose access to the District network.

- No district licensed software can or will be installed on a personal device. If an individual requires the Microsoft Office Suite, for example, they will need to purchase that through third party retailers or opt to use free suites such as Open Office or Libre Office.
- District tech support will only be provided to insure that the user is able to connect to the network.