INSTRUCTION

INSTRUCTIONAL TECHNOLOGY

Security

The District shall implement prudent security measures to ensure that only authorized individuals have access to technology equipment and resources including software applications and that such resources are physically secure.

The Director of Technology or Superintendent's Designee will have overall control of these measures. The building administrators will authorize use of technology for staff and students. Only devices approved by the Director of Technology or Superintendent's Designee and acknowledged by building level technical assistants may be connected to the network. Anyone who knows of a breach of security shall report this misuse immediately to the Building Principal or the Director of Technology or Superintendent's Designee.

Cross Reference 4510.3 INSTRUCTION
INSTRUCTIONAL TECHNOLOGY
Code of Conduct

	First	Second
Presentation: 3/4/15	Vote: 3/18/15	Vote: 4/1/15

INSTRUCTION

INSTRUCTIONAL TECHNOLOGY

Security

Security Breach

The district will maintain and follow procedures for 24/7 alarm and response monitoring of network infrastructure and firewall.

It is very important that there is no storage of any sensitive data on the local hard drive of an individual workstation. Instead, store this data on the district network server, which is assigned a greater level of security and daily backup of all files.

Sensitive data should not be copied to or stored on smartphones, disks, CD/DVDs, non-encrypted flash drives, non-district-owned/-leased computing devices, or other portable storage or computing devices. Computer applications that require the use of institutional and/or sensitive data, must access the data on the network server that is physically secured from access by unauthorized individuals, as well as protected against malicious software and unauthorized digital access.