
Each district school and Department administrator is responsible for the management and security of technology equipment and infrastructure. Administrators, in partnership with the Information Technology department (IT), must assure that:

1. All staff and all students are familiar with technology use policies and guidelines.
2. Principals and department leaders are responsible for technology planning, inventory management, equipment deployment, and assuring that staff and students follow district procedures and comply with copyright and licensure requirements.
3. Every computer is loaded with the standard district software and operating systems, and that software and operating systems are up-to-date and that the most recent security patches have been applied. Licenses for software applications that are part of the Bend-La Pine Schools standard will be maintained centrally.
4. All technology holding, purchases, donations, or acquisitions meet or exceed IT standards, are secure and supportable and may be assessed an additional charge to cover the cost of the standard software that must be installed on each computer.
5. Documents and files are located in the designated locations on staff computers and/or network file servers. This allows for file backup and computer repair while lowering the probability that school staff and students will lose critical files.
6. Software installed by school staff must be licensed (usually for every individual installation) and a record of licensure maintained by the school for inspection. Staff who purchase software and wish it installed on a district computer must donate the license to the school.
7. All technology equipment must be in working condition or must be submitted for repair as soon as a malfunction is apparent.
8. Only devices approved by IT are connected to the district network (wired or wireless) or given access to district resources. No unauthorized networking equipment, wireless access points, hotspots or wireless capable devices are installed or in use.
9. All approved devices must be connected to the network to permit upgrades, virus protection, and software/hardware auditing and inventory management.
10. Devices, software and operating systems that are no longer supported by the vendor, do not meet security standards or are otherwise un-supportable are removed from inventory and not connected to the network or other district infrastructure.
11. Only certified, low-voltage cable installers that are coordinated or hired by IT may install or repair network cable, outlets or devices. Only IT staff may install or configure network equipment,

including, but not limited to routers, switches, projectors, cameras, card locks, televisions and access points.

12. All connections and connectivity including, but not limited to phones, internet, networks, and mobile communications, are installed, managed and maintained by IT.
13. All IT closets remain secure and free from non-IT related items or activity.
14. Any technology related purchases (software and hardware) are made by, or coordinated by IT and will follow processes in [DJC-AR: Purchasing Authority and Limits](#).
15. Routine audits of school compliance with the guidelines will be made and this information will be provided to the principal or department supervisor for action as necessary.

END OF REGULATION

Reviewed: 4/7/08, 1/28/18
Approved by Cabinet: 4/7/08, 2/7/18