Arizona CTE

Technology Devices Maintenance

APPLY PROBLEM-SOLVING AND CRITICAL THINKING TO MAINTAINING TECHNOLOGY DEVICES 1.0	**1.1** Assess the technology environment (e.g., software, devices, operating systems, and device compatibility) 1.1
	1.2 Identify common project management concepts and limitations (e.g., project management triangle, goals, Gantt charts, and user needs) 1.2
	1.3 Determine priorities in establishing and maintaining computers/electronic devices (i.e., user needs, workflow, data security, etc.) 1.3
	1.4 Apply problem-solving processes to computers and electronic devices (i.e., define problem, identify cause, research problem, select and test solution, prevent the problem, etc.) 1.4
	1.5 Document the results and update the problem-solving process 1.5
MAINTAIN A SAFE AND ENVIRONMENTALLY CONCIOUS TECHNOLOGY WORKPLACE 2.0	**2.1** Identify and apply personal responsibility for a safe and healthy environment (i.e., conforming to industry standards, recycling protocols for toxic/non-toxic materials, avoid/eliminate electrical hazards, etc.) 2.1
	2.2 Use job-specific tools, materials, and equipment used to maintain technology 2.2
	2.3 Identify ergonomics and repetitive strain injuries experienced in technology maintenance occupations 2.3
	2.4 Explain various safety measures and procedures including electrostatic discharge and how inadequate measures can damage equipment 2.4
ADDRESS SECURITY ISSUES RELATED TO TECHNOLOGY DEVICES 3.0	**3.1** Identify security issues related to the technology environment (i.e., computer hardware and software, data, mobile devices, networks, etc.) 3.1
	3.2 Identify and apply or create and update policies to maintain data integrity and security 3.2
	3.3 Explain the importance of physical security of computer hardware and electronic devices 3.3
	3.5 Identify methods to protect and prevent security threats 3.5

	3.4 Explain user-related threats (i.e., ransomware, phishing, viruses, email attachments, social engineering, spoofing, identify theft, spamming, etc.) 3.5 Identify methods to protect and prevent security threats 3.4
	3.6 Explain external threats (i.e., denial of service, hacking/cracking, intrusion, etc.) 3.6
EXPLORE LEGAL AND ETHICAL ISSUES RELATED TO INFORMATION TECHNOLOGY 4.0	**4.1** Identify issues specific to intellectual property rights including copyright, software licensing, patents, software piracy, and software duplication 4.1
	4.2 Identify issues and trends affecting data and information privacy 4.2
	4.3 Differentiate between ethical and unethical uses of technology (i.e., black hat/white hat hacking, industry-specific restrictions, etc.) 4.3
	4.4 Identify workplace issues created by improper use of technology (i.e., cyberbullying, discrimination, social posts, trolling, privacy, etc.) 4.4
EXPLORE RAMIFICATIONS OF TECHNOLOGY DEVELOPMENT 5.0	**5.1** Explore challenges regarding the evolution of technology and their impact on our lives (i.e., automation, shift in occupations, data compatibility, security, privacy, consumer history, etc.) 5.1
	5.2 Explore future trends in technology with positive and negative implications 5.2
	5.3 Explore methods for keeping up with technology changes (i.e., forums, newsletters, Google alerts, technology announcements, etc.) 5.3
INSTALL, CONFIGURE, UPGRADE, AND MAINTAIN TECHNOLOGY	**6.1** Identify the purpose and characteristics of common system components (i.e., storage devices, power supply, removable media, expansion cards, memory, etc.) 6.1
	6.2 Identify the purpose and characteristics of mobile device components (i.e., power supply, removable media, screens, batteries, speakers, ports, etc.) 6.2
	6.3 Demonstrate basic procedures for adding and removing common system components and recognizing associated cable connections 6.3
	6.4 Distinguish the names, purposes, and performance characteristics of common peripheral ports 6.4
	6.5 Demonstrate proper procedures for installing and configuring common peripheral devices 6.5
	6.6 Identify issues that must be considered when upgrading technology components [i.e., safety (electrical), data integrity, compatibility, user privacy, etc.] 6.6

	6.7 Follow procedures for preventive maintenance of computers and peripherals (i.e., physical cleaning, defragmenting drives, data backup, security updates, etc.) 6.7
	6.8 Determine the cost-benefit of replacement or repair of hardware/software 6.8
ASSESS MOTHERBOARDS, PROCESSORS, AND MEMORY	**7.1** Identify CPU chip types, manufacturers, and associated sockets 7.1
	7.2 Distinguish differences between surface mount technology (SMT) and socketed components 7.2
	7.3 Identify operational characteristics of RAM (e.g., speed, type, and size) 7.3
	7.4 Identify the responsibility of the various components of the motherboard (i.e., integrated ports, expansion slots, chipsets, battery, etc.) 7.4
	7.5 Identify basic compatibility guidelines of the motherboard, processors, and memory 7.5
	7.6 Explain the role of BIOS and CMOS in computer technology 7.6
	7.7 Explain how environmental factors including heat, airborne particulates, humidity, vibration, and shocks can affect equipment 7.7
	7.8 Explain the relationship of hertz to processor and bus speeds 7.8
	7.9 Explain the relationship of bits and bytes to common memory and storage capacities 7.9
	7.10 Apply basic electronics theories (i.e., Ohm's Law, calculation of wattage, voltage, amperage, resistance, capacitance, etc.) 7.10
INSTALL AND MAINTAIN PRINTERS AND SCANNERS	**8.1** Compare and contrast printer technologies including laser, ink dispersion, solid ink, thermal, impact, and dye sublimation 81
	8.2 Explore connection options for each printer and scanner technology (i.e., wired vs wireless, server interface, cable types, local infrastructures, etc.) 8.2
	8.3 Determine options to upgrade printers (i.e., memory, hard drives, NICS, FAX, etc.) 8.3
	8.4 Troubleshoot common printer problems (i.e., paper jam, connectivity, consumables, power, security protocols, etc.) 8.4
EXPLAIN BASIC NETWORKING HARDWARE	**9.1** Differentiate common types of network cables, topologies, and their characteristics 9.1
	9.2 Install and configure network cards and adapters 9.2

	9.3	Differentiate common technologies available for establishing network connectivity (i.e., routers, wireless, hubs, modem, switches, repeaters, mesh networks, etc.) 9.3
	9.4	Diagnose simple hardware problems in networking equipment (i.e., interpret error codes/messages, etc.) 9.4
COMPARE THE BASICS OF COMMON OPERATING SYSTEMS	10.1	Differentiate the characteristics of common device operating systems (i.e., Windows, IOS, Android, Linux, MAC, etc.) 10.1
	10.2	Distinguish major software features and functions by device (i.e., taskbar, menus, notification bars, gestures, etc.) 10.2
	10.3	Navigate major operating system management tools (i.e., file management, administrative tools, command line, REGEDIT, Task Manager, system utilities, etc.) 10.3
	10.4	Explain command-line functions and utilities to manage the operating system including the proper syntax and switches (i.e., file attributes, commands for creating, viewing, and managing drives, directories, files, etc.) 10.4
	10.5	Identify common data redundancy options (i.e., network attached storage, RAID, cloud storage, etc.) 10.5
INSTALL, CONFIGURE, AND UPDATE OPERATING SYSTEMS	11.1	Compare and contrast the differences between native and virtualized operating system environments 11.1
	11.2	Install operating systems using default and customized installation options 11.2
	11.3	Backup and restore user data (i.e., copy/paste, images, clones, etc.) 11.3
	11.4	Identify common symptoms and resolve problems encountered during installations and version upgrades 11.4
	11.5	Perform operating system updates 11.5
	11.6	Set up basic system boot sequences and boot methods including recovery options 11.6
	11.7	Install and add a device by installing and configuring device drivers and required software 11.7
	11.8	Optimize the operating system (i.e., deleting temporary files, user needs, custom startup settings, built-in optimization tools, etc.) 11.8
	11.9	Perform cross-platform migration retaining user data and settings (i.e., computers, tablets, smartphones, etc.) 11.9

	11.10	**Interpret the meaning of common error codes and startup messages from the boot sequence and identify steps to correct problems** 11.10
	11.11	**Apply common diagnostic utilities and tools** 11.11
TROUBLESHOOT A NETWORK	**12.1**	**Assess the networking capabilities of common operating systems (i.e., domain, workgroup, etc.)** 12.1
	12.2	**Determine best protocols and encryption levels (i.e., TCP/IP, NetBIOS, wireless encryption, etc.)** 12.2
	12.3	**Use network troubleshooting applications (i.e., IPCONFIG, PING, TRACERT, NSLOOKUP, DIG, NETSTAT, NBTSTAT, ARP, etc.)** 12.3
	12.4	**Define basic internet protocols and terminologies (i.e., HTTP, HTTPS, FTP, SMTP, DNS, DHCP, POP, etc.)** 12.4
	12.5	**Identify infrastructure and procedures for establishing internet connectivity 12.6 Configure software/hardware firewall protection** 12.5
	12.6	**Configure software/hardware firewall protection** 12.6