Open Awards

Unit

Form OAQU

1 Unit Details

Unit Title:	Understanding PC Technology
Unit Code:	CJ7/3/WR/001
Level:	Level 3
Credit Value:	8

2 Learning Outcomes and Criteria

Learning Outcome (The Learner will):	Assessment Criterion (The Learner can):
1. Understand the function of the major internal PC hardware components and peripheral devices.	1.1 Describe all of the PC's major internal components, including: a) System unit; b) Central processing unit; c) Motherboard; d) System memory; e) Hard disk drives; f) Power Supply; g) Cooling systems; h) Expansion Cards; and i) Built-in ports.
	1.2 Describe the function of the following motherboard components and how they interact with each other: a) Central Processing Unit;; b) Chipset; c) Front-side bus; d) Back-side bus; e) Cache memory; f) System clock; g) Read-only memory; h) Random access memory; and i) BIOS or UEFI firmware.

	1.3	Describe the function and the underlying technologies of the following peripheral devices a) Keyboards; b) Pointing devices; c) Security devices; d) Display monitors; e) Touch screens; f) Printers; and g) Multi-function devices.
2. Understand how to install and configure the major PC hardware components.	2.1	Recognise and describe the underlying display device technologies and hardware connectors, and how they are installed and configured in Windows.
	2.2	Recognise and describe the various keyboard and mice technologies and how they are installed and configured in Windows.
	2.3	Describe the various printer and scanner technologies and how they are installed and configured in Windows.
	2.4	Recognise and describe the use of the various expansion card types, and be able to install and configure them.
	2.5	Describe the different types of CPU and how to install and configure them, along with their cooling fans.
	2.6	Install and connect a PC power supply.
	2.7	Install and configure Random Access Memory.
	2.8	Install, initialise, partition, and format a hard disk drive.
3. Understand how to diagnose and resolve PC hardware problems, and design and implement a preventative maintenance schedule.	3.1	Troubleshoot and resolve problems with internal PC components, including: a) Central Processing Units; b) The BIOS or UEFI firmware; c) Cooling systems; d) Various motherboards; e) Power supplies; and f) Boot failure;
	3.2	Describe common disk drive errors, and troubleshoot and resolve said problems.
	3.3	Utilise specialist diagnostic software.
	3.4	Implement a wide range of preventative maintenance procedures.

4.	Understand how to support a wide range of mobile devices, including laptop computers, tablet computers, and smartphones.	4.1	Describe the underlying technology of the following laptop components: a) Motherboard and its components; b) Various types of CPU; c) Random Access Memory; d) Disk drives; e) Keyboards; f) Touchpads; g) Optical disks; and h) Display screens.
		4.2	Create and implement a laptop maintenance schedule, including battery care guidelines.
		4.3	Describe the major components and underlying technology of various types of tablet computers and smartphones.
		4.4	Troubleshoot common mobile device problems, including wireless issues.
5.	Understand the major local and wide area network hardware components, network protocols, and maintenance procedures.	5.1	Describe the functionality of the following network components: a) Network interface cards; b) Network cables; c) Hubs; d) Switches; e) Routers; f) Bridges; g) Gateways; and h) Repeaters.
		5.2	Describe the following network protocols: a) TCP/IP; b) Data packet structure and delivery; c) IP addresses; d) Network Address Translation; e) Domain name servers. f) User Datagram Protocol; g) LDAP directory services; and h) Simple Network Management Protocol.
		5.3	Describe the underlying technology of the Internet, including the various broadband access methods, and security threats.
		5.4	Use a wide range of networking diagnostic tools to troubleshoot errors and security threats.
6.	Understand the Windows operating system structure and components, and be able to install and configure Windows.	6.1	Create Windows installation media and perform and configure both a clean Windows 10 installation and an upgrade from an earlier version.

	6.2	Describe and configure the Windows Start Menu, Taskbar, and Desktop, including: a) Frequently used apps; b) Managing app tiles; c) The Quick Access menu; d) Access to All Apps; e) Pinning to the taskbar; f) Adding toolbars; g) Taskbar icons; h) Keyboard shortcuts; i) Maintaining virtual desktops; and j) Personalising the desktop.
	6.3	Utilise the Clipboard, Recycle Bin, and File Explorer.
	6.4	Describe and utilise the major Control Panel features, including: a) Security & Maintenance; b) Speech Recognition; c) Default programs; d) Administrative Tools; e) Device Manager; f) Network & Sharing; g) Personalisation; and h) Troubleshooting.
	6.5	Describe and utilise the important Windows Accessories, including: a) Notepad; b) WordPad; c) Paint; d) Fax & Scan; and e) Windows Media Player.
7. Understand the importance of the Windows operating system maintenance procedures.	7.1	Configure and schedule the built-in Windows automatic maintenance procedures.
	7.2	Implement Windows optimisation and performance-enhancing procedures.
	7.3	Implement data backup and recovery procedures.
	7.4	Implement disk storage maintenance using the range of built-in Windows utilities.
	7.5	Install Windows software updates.
8. Recognise common security threats and take appropriate steps to combat them.	8.1	Describe the threats posed by various types of malware, including: a) Viruses; b) Worms; c) Trojan horses; d) Logic bombs; e) Spyware; f) Phishing; g) Spoofing;

		h) Sniffing; and i) Denial of service.
	8.2	Describe and implement security “best practices” in a formal Security Policy;
	8.3	Describe and install hardware and software firewalls, and intrusion detection systems.
	8.4	Describe the security threats posed to mobile devices and take appropriate action to prevent them.
	8.5	Describe and configure the Windows built-in security features including Windows Defender and Windows Firewall.
	8.6	Counteract the security threats posed to wired and wireless networks.