3.5 Fundamentals of computer networks

3.5.1 Network basics

Content	Additional information	Chk
Define what a **computer network** is. Discuss the advantages and disadvantages of computer networks.		
Describe the main types of computer network including: • Personal Area Network (PAN) • Local Area Network (LAN) • Wide Area Network (WAN).	PAN – only Bluetooth needs to be considered. LAN – know that these usually cover relatively small geographical areas. LAN – know that these are often owned and controlled/managed by a single person or organisation. WAN – know that the Internet is the biggest example of a WAN. WAN – know that these usually cover a wide geographic area. WAN – know that these are often under collective or distributed ownership.	
Understand that networks can be **wired** or **wireless**. Discuss the advantages and disadvantages of wireless networks as opposed to wired networks.	Know that wired networks can use different types of cable such as fibre and copper and when each would be appropriate.	
Describe the following common LAN **network topologies**: • star • bus.	Students should be able to draw topology diagrams and describe the differences between the two topologies. They should also be able to select the most appropriate topology for a given scenario.	

3.5.2 Network protocols

Content	Additional information	Chk
Define the term **network protocol**.		
Explain the purpose and use of common network protocols including: • Ethernet • Wi-Fi • TCP (Transmission Control Protocol) • UDP (User Datagram Protocol) • IP (Internet Protocol) • HTTP (Hypertext Transfer Protocol) • HTTPS (Hypertext Transfer Protocol Secure)	Students should know what each protocol is used for (eg HTTPS provides an encrypted version of HTTP for more secure web transactions). Students should understand that Ethernet is a family of related protocols rather than a single protocol. They do not need to know the individual protocols that make up the Ethernet family.	

• FTP (File Transfer Protocol)
• email protocols:
  ○ SMTP (Simple Mail Transfer Protocol)
  ○ IMAP (Internet Message Access Protocol).
	Students should understand that Wi-Fi is a family of related protocols rather than a single protocol. They do not need to know the individual protocols that make up the Wi-Fi family but they should know that Wi-Fi is a trademark and that the generic term for networks of this nature is WLAN.	

Describe the **4 layer TCP/IP model**: • application layer • transport layer • internet layer • link layer. Understand that the HTTP, HTTPS, SMTP, IMAP and FTP protocols operate at the application layer. Understand that the TCP and UDP protocols operate at the transport layer. Understand that the IP protocol operates at the internet layer.	Students should be able to name the layers and describe their main function(s) in a networking environment. Application layer: this is where the network applications, such as web browsers or email programs, operate. Transport layer: this layer sets up the communication between the two hosts and they agree settings such as 'language' and size of packets. Internet layer: addresses and packages data for transmission. Routes the packets across the network. Link layer (network layer): this is where the network hardware such as the NIC (network interface card) is located. OS device drivers also sit here.	

3.5.3 Network security

Content	Additional information	Chk
Understand the need for, and importance of, **network security**.		
Explain the following methods of network security: • authentication • encryption • firewall • MAC address filtering.	Students should be able to explain, using examples, what each of these security methods is and when each could be used. Students should understand how these methods can work together to provide a greater level of security. A firewall is a network security device that monitors incoming and outgoing network traffic and decided whether to allow or block specific traffic based on a defined set of security rules. Students should understand that MAC address filtering allows devices to access, or be blocked from accessing a network based on their physical address embedded within the device's network adapter.	