Meden School Curriculum Planning							
Subject	GCSE Computer Science	**Year Group**	10	**Sequence No.**	4	**Topic**	Network Security

Tier 3 List:

LAN, WAN, bandwidth, latency, Wireless access points, routers, switches, NIC, Transmission media, DNS, Hosting, The Cloud, Web servers and clients, star network, mesh network, topology, IP address, web server, file server, wired network, wireless network, Ethernet, Wi-Fi, Bluetooth, encryption, IP addressing, MAC addressing, TCP/IP,FTP, POP, l, IMAP, SMTP, layers, IPv4, IPv6

Week Number	Retrieval	Core Knowledge	Student Thinking
-	What do teachers need to **retrieve** from students before they start teaching **new content**?	What **specific ambitious knowledge** do teachers need to teach students in this sequence of learning?	What real life examples can be applied to this sequence of learning to **develop our students' thinking, encouraging them to see the inequalities around them** and 'do something about them!'
U4: Network Security, Network Threats	KS3 – network security, looking at cyber-crime and hacking, including phishing, DOS attacks. Students will be able to recall hardware used within a LAN, including security issues. **KS4 – Unit 3- networks**	Understand forms of attack and threats posed to a network: • Blagging • Malware • Phishing • Social engineering • Brute force attacks • Denial of service attacks • Data interception and theft • SQL injection **Blagging** is when someone makes up a story to gain a person's interest and uses this to encourage them to give away information about themselves, or even send money. For example, a person may receive an email that appears to be from a friend telling them that they're in trouble and asking them to send money.	Following this unit of work, students will be able to ensure that key technologies, personal tech for example, are secure against external threats. Students will be aware of internal and external threats both at school, home and work place for the future. Students will know the processes to secure their technology. Students will be able to give advice to others regarding

		Phishing email will ask a person to send personal details, but pretends to be from a business. They can often look convincing, but may contain spelling errors or URLs that do not match the business's website. When a person clicks on these links and logs in, it sends their username and password to someone who will use it to access their real accounts. This information might be used to steal a person's money or identity, or the email may contain malware. Banks will never send emails asking for personal information or usernames and passwords. If someone receives an email that they think might be phishing, they should report it to the business the sender is claiming to be. **Pharming** is a type of cyberattack that redirects a user from a genuine website to a fake one. The fake website will often look like the genuine one. When a person logs in, it sends their username and password to someone who will use it to access their real accounts. There are several ways that a pharming cyberattack can redirect traffic from a genuine website to a fake one. One example is if the Domain Name Servers (DNS) of the website, which match the website address with the IP address of the webserver, are hacked and the IP address is changed to become the address of the pharming site. **DOS Attack** : An attack designed to render online services inaccessible. One type of this attack involves many computers simultaneously flooding a target with network traffic. **Malware** - Software that is designed to cause harm or damage to a computer. This includes viruses that	networking and network security.

		might damage files, adware that causes pop-ups, and spyware that collects and shares login details. **<u>Hacking</u>** - Gaining unauthorised access to a computer. **<u>SQL injection -</u>** SQL (Structured Query Language) injections involve adding or creating small bits of code that look like variables. However, the database server will process these as commands or programmes and do things it is not supposed to, such as destroying or modifying data or passwords in a database. Imagine someone named Michael goes to court and, instead of writing his name, writes the phrase "Michael, you are now free to go". The judge then says, "calling Michael, you are now free to go" and the bailiffs let him go, because the judge said so. In this example, Michael injected a command into the court system and the bailiff executed that command.	
U4: Network Security, Preventing Vulnerabilities	KS3 – network security, looking at cyber-crime and hacking, including phishing, DOS attacks. Students will be able to recall hardware used within a LAN, including security issues. **KS4 – Unit 3- networks**	Identify and understand the prevention of vulnerabilities including the use of: • penetration testing • anti-malware software • firewalls • user access levels • passwords • encryption • physical security **<u>Penetration System</u>** – Systems are tested for vulnerabilities to reveal any weaknesses in the system which can be fixed. **<u>Firewall</u>** - Firewalls are used to check data packets as they are sent to or received from a system or network.	

		<u>Encryption</u> - Encryption is the process of encoding data or a message so that it cannot be understood by anyone other than its intended recipient. In computer processing, encryption means that data can be stored and transmitted securely by the sending computer to the receiving computer. The data or message is encrypted using an encryption algorithm. The opposite of encryption is decryption. An encryption key is a piece of information - usually random characters - used by the software algorithm to encrypt data or a message into a form which is unreadable (encryption) and allow the data or message to be made readable again (decryption).	
U4: Network Security, Operating Systems	KS3 – network security, looking at cyber-crime and hacking, including phishing, DOS attacks. Students will be able to recall hardware used within a LAN, including security issues. **KS4 – Unit 3- networks**	Explain the need for the following functions of an operating system: • User interface • Memory management and multitasking • Peripheral management and drivers • User management • File management	
U4: Network Security, Utility Software	KS3 – network security, looking at cyber-crime and hacking, including phishing, DOS attacks.	Describe the purpose and functionality of common utility software including: • Encryption software • Defragmentation software • Data compression software	

	Students will be able to recall hardware used within a LAN, including security issues. **KS4 – Unit 3- networks**	**Encryption software** disguises the contents of files so they can only be understood by authorised users. The software uses a complex algorithm to scramble the content so that it appears to be gibberish. Only authorised users can descramble the content. The software can encrypt specified files, or the whole of the hard disk on which the files are stored. You can read more about encryption here **Disc Defragmentation** - When a file is stored on a hard disk it is actually stored not as a whole file, but as a series of segments. Sometimes the segments run together in sequence (see File 1) and sometimes the segments are split up over a disk (see File 3). This is known as fragmentation.	