Curriculum Sequencing - Year 9

Year 9 Term 1a:	
Topics covered:	Introduction & Cybersecurity
How it links to what has been studied before:	At the heart of cybersecruity is esafety and this specific topic is crucial to cybersecurity.
How it links to what will be studied:	Understand a range of ways to use technology safely, respectfully, responsibly, and securely, including protecting their online identity and privacy; recognise inappropriate content, contact, and conduct, and know how to report concerns
Key words:	Brute force attack, Common malware threats, Computer Misuse Act, Cyber security, Cyberattacks, Data, Data compromised, Data privacy, Data Protection Act, Data Strategies, DDoS attack, Hacking,Human errors, Information, Malicious bots, Networks, Online services, Organisations, Protected, Security risks, Security threats, Societal issues, Users
Assessment focus	Lesson 1 = Computer Science Baseline, Lessons 2-5 have an a formative assessment. Lesson 6 is a summative assessment.
Revision tips	Revise the content from the lesson slides and exit tickets. BBC Bitesize Revision
Key skills:	Explain the difference between data and information Critique online services in relation to data privacy Identify what happens to data entered online Explain the need for the Data Protection Act Recognise how human errors pose security risks to data Implement strategies to minimise the risk of data being compromised through human error Define hacking in the context of cyber security Explain how a DDoS attack can impact users of online services Identify strategies to reduce the chance of a brute force attack being successful Explain the need for the Computer Misuse Act List the common malware threats Examine how different types of malware causes problems for computer systems Question how malicious bots can have an impact on societal issues Compare security threats against probability and the potential impact to organisations Explain how networks can be protected from common security threats Identify the most effective methods to prevent cyberattacks
Why we study it:	This unit takes the learners on an eye-opening journey of discovery about techniques used by cybercriminals to steal data, disrupt systems, and infiltrate networks
Mastery in this subject	Elaborate on the distinction between data and information, highlighting the transformative process through which raw data acquires meaning and significance. Evaluate online services from the perspective of data privacy, critically

	analyzing their practices and policies to safeguard user data and personal information. Investigate the outcomes of data submitted online, exploring how it is collected, stored, processed, and potentially shared by various digital platforms and services. Justify the necessity of the Data Protection Act, emphasizing its role in safeguarding individuals' privacy and ensuring responsible handling of personal data by organizations. Assess the security risks posed by human errors, recognizing how inadvertent actions or oversight can lead to data vulnerabilities and potential breaches. Devise and implement effective strategies to mitigate the risk of data compromise resulting from human error, emphasizing best practices and proactive measures. Define hacking within the context of cybersecurity, elucidating the techniques used by malicious actors to exploit vulnerabilities and gain unauthorized access to computer systems. Examine the impact of Distributed Denial of Service (DDoS) attacks on users of online services, considering the disruptions caused by overwhelming network traffic and the resulting implications. Analyse various strategies aimed at reducing the likelihood of a successful brute force attack, emphasizing the importance of robust password policies and authentication mechanisms. Articulate the significance of the Computer Misuse Act, outlining how it deters and prosecutes unauthorized access, misuse, or interference with computer systems and data. Enumerate and classify common malware threats, describing their characteristics and potential consequences for computer systems and users. Evaluate the multifaceted problems caused by different types of malware on computer systems, considering the scope of damages and potential countermeasures. Investigate the societal impact of malicious bots, exploring how these automated agents can affect various domains, including cybersecurity, social media, and economic systems. Conduct a comparative analysis of security threats, considering both their probability of occurrence and the potential impact they pose to organizations, to prioritize risk management efforts. Elucidate strategies for safeguarding networks against common security threats, encompassing approaches such as firewalls, intrusion detection systems, and security protocols. Identify and elaborate on the most effective methods to prevent cyberattacks, including advanced threat detection, timely software updates, employee training, and proactive security measures.
Year 9 Term 1b:	
Topics covered:	Layers of Computing Systems
How it links to what has been studied before:	Data representations and Networks

How it links to what will be studied:	Computer systems utilize data representation to store, process, and retrieve information, while networks enable communication and data exchange between interconnected systems.
Key words:	AND Artificial intelligence Computing systems Construct Execute programs Function Gathering data General-purpose computing system Hardware components Logic circuits Logical expressions Logical operators Machine learning NOT OR Purpose-built device Real world Testing
Key skills:	Differentiate general-purpose computing systems from purpose-built devices. Understand the function of hardware components in computing systems. Comprehend how hardware components collaborate to execute programs. Analyze the collaboration of hardware components in program execution. Understand NOT, AND, and OR logical operators and their use in logical expressions. Understand logic circuits, logic gates, and their association with operators and expressions. Describe the construction of hardware using complex logic circuits. Confidently explain real-world examples of artificial intelligence and machine learning. Describe the steps in training machines (data gathering, training, testing). Differentiate machine learning from traditional programming. Consider the ethical implications of artificial intelligence. Understand the consequences of sharing program code.
Assessment focus	Each lesson has an exit ticket as a formative assessment. The last lesson of the term is a summative assessment.
Revision tips	Revise the content from the lesson slides and exit tickets. BBC Bitesize Revision
Why we study it:	● Understand and apply the fundamental principles and concepts of computer science, including abstraction, logic, algorithms and data representation ● Evaluate and apply information technology, including new or unfamiliar technologies, analytically to solve problems

Mastery in this subject	Confidently explain the difference between a general-purpose computing system and a purpose-built device Describe the function of the hardware components used in computing systems Describe how the hardware components used in computing systems work together in order to execute programs Analyse how the hardware components used in computing systems work together in order to execute programs Describe the NOT, AND, and OR logical operators, and how they are used to form logical expressions Construct logic circuits using logic gates, and associate these with logical operators and expressions Describe how hardware is built out of increasingly complex logic circuits Confidently explain examples of artificial intelligence and machine learning in the real world Describe the steps involved in training machines to perform tasks (gathering data, training, testing) Describe how machine learning differs from traditional programming Debate the use of artificial intelligence with moral dilemmas Explain the implications of sharing program code