KESTEVEN AND SLEAFORD HIGH SCHOOL

Computer Science Scheme of Learning

Year 11 – Term 4

Intent – Rationale

Term 2 continues to focus on networking, focusing more specifically on the role or wired and wireless technologies, before switching to the final topic of the course: Threats to IT Systems.

Sequencing – what prior learning does this topic build upon?	Sequencing – what subsequent learning does this topic feed into?
• Year 9 Topic 6	• A-Level Computer Science Chapters 16 and 18
What are the links with other subjects in the curriculum?	**What are the links to SMSC, British Values and Careers?**
• N/A	• M1, BV2
What are the opportunities for developing literacy skills and developing learner confidence and enjoyment in reading?	**What are the opportunities for developing mathematical skills?**
• *Cybercrime & Digital Forensics: An Introduction.* 2017 by Thomas J. Holt et al • *Crime Dot Com: From Viruses to Vote Rigging, How Hacking Went Global.* 2020. by Geoff White	• N/A

KESTEVEN AND SLEAFORD HIGH SCHOOL

Computer Science Scheme of Learning

Year 11 – Term 4

Intent – Concepts

What knowledge will students gain and what skills will they develop as a consequence of this topic?	
Know • **Wired and wireless networks, protocols and layers**: modes of connection (wired Ethernet, wireless, Wi-Fi, Bluetooth), the role of encryption, IP and MAC addressing, standards • **Threats**: Forms of attack: Malware, Social engineering, e.g. phishing, people as the 'weak point', Brute-force attacks, Denial of service attacks, Data interception and theft, and the concept of SQL injection • **Common prevention methods:** Penetration testing, Anti-malware software, Firewalls, User access levels, Password, Encryption and Physical security **Apply** • Be able to compare benefits and drawbacks of wired versus wireless connection and recommend one or more connections for a given scenario • Be able to describe the principle of encryption to secure data across network connections, and the role of IP addressing (ipv4 and ipv6) and MAC addressing • Ba able to describe threats posed to devices/systems including how the attack is used and the purpose of the attack • Be able to identify how to limit the threats posed including an understanding of methods to remove vulnerabilities, knowledge/principles of each prevention method, what each prevention method may limit/prevent and how it limits the attack **Extend** • Active participation in Cyber Discovery	
What subject specific language will be used and developed in this topic?	**What opportunities are available for assessing the progress of students?**

KESTEVEN AND SLEAFORD HIGH SCHOOL

• Ethernet • Wireless • Channel • Interference • Contention ratio • Bluetooth • Encryption • Symmetric • Asymmetric • Cloud •	• Malware • Social engineering • Phishing • Brute-force attacks • Denial of service attacks • Data interception • SQL injection • Penetration testing • Anti-malware software • Firewalls • User access levels • Passwords • Encryption • Physical security	• Class Notes and in-lesson observation • Kahoot starters/plenaries and verbal questioning • Formal assessment in scheduled weeks

Intent – Concepts

Lesson title	Learning challenge	Higher level challenge	Suggested activities and resources
			See P drive for lesson presentations/resources