YEAR 11 (IT) HALF TERM 1.2

MAGHULL HIGH SCHOOL – CURRICULUM MAP

Unit: Effective Digital Working Practices	Week 1	Week 2	Week 3	Week 4	Week 5	Week 6	Week 7	Week 8
LESSON TOPIC QUESTION(S)	**Lesson 1**Why are systems attacked? **Lesson 2** What are the external threats to an organisation? **Lesson 3** How does social engineering make a system vulnerable?	**Lesson 4** How can hackers help make a system secure? **Lesson 5** How can the users cause a system to be vulnerable?	**Lesson 6** What are the internal threats to a system? **Lesson 7** What impact does a s security breach have? **Lesson 8** Can I show what I have learnt?	**Lesson 9** How can you protect a system from external threats? **Lesson 10** How can you protect a system from internal threats?	**Lesson 11** How do we protect data within a system? **Lesson 12** What areas do I need to revise? **Lesson 13** Can I show what I have learnt?	**Lesson 14** How does encryption work? **Lesson 15** What areas do I need to revise?	**Lesson 16** What are security parameters? **Lesson 17** What do you do after a cyber-attack? **Lesson 18** Can I show what I have learnt?	**Lesson 19** What areas do I need to revise?
Knowledge & Skills development	**<u>Theory Knowledge</u>** *Understand why systems are attacked* *Describe the external threats worms, botnet, rootkit, ransomware, spyware, social engineering and 'man-in-the-middle' attacks* *Understand the internal threats of stealing or leaking information, overriding security controls and downloads from the internet and untrustworthy websites* *Understand the impact of security breaches including data and financial loss* *Describe user access restrictions including physical security measures, passwords, user settings, biometrics and two-factor authentication* *Understand how computers are protected with anti-virus software, with firewalls, interface design and encryption* *Understand how backups are used to recover data* *Explain the term 'black hat' hacker, the use of ethical hacking and white hat hackers*				**<u>Digital Skills</u>** *Be able to work with multiple windows* *Be able to access Teams and complete work* *Be able to access the MS365 suite of apps* *Use common shortcut keys* *Research and development of solutions to problems*			

Assessment / Feedback Opportunities	***Formative Assessment*** Class activity Class Discussion Questioning pupils Verbal Feedback Live Marking	***Summative assessment*** Knowledge Checks Cumulative Assessment
Key Vocabulary	Hacker, system attack, black hat, white hat, grey hat, malware, virus, worm, botnet, rootkit, Trojan, ransomware, spyware, Denial of Service, phishing, pharming, social engineering, shoulder surfing, 'man-in-the-middle' attacks, unintentional disclosure, information theft, security controls, security breach, internal threat, passwords, access levels, biometrics, two-factor authentication, ethical hacking, penetration testing, system analysis, behaviour analysis, firewall, interface design, autocomplete, anti-virus, device hardening, encryption, cyber security, policy, acceptable use policy (AUP), disaster recovery, backups	
Literacy/Reading opportunities	**Books** The Coming Wave: AI, Power and Our Future The Teenage Guide to Digital Wellbeing **Refactoring UI** **Website for technology news** https://newsforkids.net/category/all_news/science/technology/ https://www.dogonews.com/category/technology	
Cross Curricular Themes	Development of digital skills and use of online platforms	
Personal Development (Including British Values, RSE, Citizenship)	Respectful communication	
Career Opportunities	Network Administrator – Network System Engineer - Network Programmer/Analyst - Network Systems Manager – Cyber Security	