



MAGHULL HIGH SCHOOL – CURRICULUM MAP

HALF TERM 2.1 Jan - Feb	Component 3 Learning Aim A: Section 4	Component 3 Learning Aim A: Assessment	Component 3 Learning Aim B: Section 1	Component 3 Learning Aim B: Section 2	Component 3 Learning Aim B: Section 3
TOPIC (S)	Impact of modern technologies	Assessment	Cyber Security: External and Internal Threats	Cyber Security: Impact of breach	Cyber Security: Prevention of threats
Knowledge & Skills development	Understand the positive and negative impact that the use of modern technologies has on organisations and stakeholders.	Demonstration of theory learnt in the unit of study	Understand why systems are attacked, the nature of attacks and how they occur Understand the potential impact of breaches in security on the organisation and stakeholders. Understand how different measures can be implemented to protect digital systems. Understand the purpose of different systems and how their features and functionality protect digital systems.		
Assessment / Feedback Opportunities	Classroom activity - Class Discussion - Questioning pupils – verbal feedback – exam questions – end of section tests	Written Assessment	Classroom activity - Class Discussion - Questioning pupils – verbal feedback – exam questions – end of section tests		
Cultural Capital	<ul style="list-style-type: none">• Variations of technology• Global Technology and Society				
SMSC / Promoting British Values (Democracy, Liberty, Rule of Law, Tolerance & Respect)	<ul style="list-style-type: none">• Listening to others• Responding suitable in discussions• Taking part in group activities				
Reading opportunities	Explain the cloud like I am 10 Networking made easy All in one networking		Ghost In The Wires Social Engineering Hacking: The Art of Exploitation The Science of Secrecy from Ancient Egypt to Quantum Cryptography		
Key Vocabulary	Ad hoc networks – network availability – synchronisation – scalability – collaboration tools – interface design – notifications – disaster recovery – compatibility – downtime – collaboration tools – communication tools – scheduling and planning tools – communication platforms – communication channels – infrastructure		industrial espionage – malware – DOS – phishing – pharming – social engineering – shoulder surfing – data loss – downtime – password – two factor authentication – biometrics – firewall – device hardening – encryption – ethical hacking – penetration testing		
Digital Literacy	Use of technology Digital research methods Use of range of software				

Careers	IT manager – Network manager – System analyst – Cyber security – White hat hacking – System testing – Software engineer
---------	---