HALF TERM 2.2 Feb - Apr	Component 3 Learning Aim B: Section 4	Component 3 Learning Aim B: Section 5	Component 3 Learning Aim B: Assessment	Component 3 Learning Aim C: Section 1	Component 3 Learning Aim C: Section 2	Component 3 Learning Aim C: Section 3
TOPIC (S)	Cyber Security: Management of threats	Cyber Security: Policies	Assessment	The implications of digital systems: Responsible use	The implications of digital systems: Legal	The implications of digital systems: Ethical
Knowledge & Skills development	Understand how one or more systems or procedures can be used to reduce the nature and/or impact of threats Understand the need for and nature of security policies in organisations		Demonstration of theory learnt in the unit of study	Understand the responsible use of digital systems, including how systems and services share and exchange data as well as the environmental considerations of increased use. Understand the scope and purpose of legislation that governs the use of digital systems and data. Understand the wider ethical considerations of use of technologies, data and information.		
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	• Variations of technology • Global Technology and Society					
SMSC / Promoting British Values (Democracy, Liberty, Rule of Law, Tolerance & Respect)	• Listening to others • Responding suitable in discussions • Taking part in group activates					
Reading opportunities	Ghost in The Wires Social Engineering Hacking: The Art of Exploitation The Science of Secrecy from Ancient Egypt to Quantum Cryptography					
Key Vocabulary	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			Shared data – location based data – transactional data – cookies – data exchange – digital systems – power-saving – electronic distribution – net neutrality – Scope – assets – monitoring – sanctions – Data protection – right to be forgotten – Intellectual property – malware		
Digital Literacy	Use of technology Digital research methods Use of range of software					
Careers	System analyst – Cyber security – White hat hacking – System testing – Software engineer					