




# YEAR 11 GCSE COMPUTER SCIENCE AUTUMN TERM 1 – PAPER 1

'An ambitious curriculum that meets the needs of all'

## Medium Term Planning – Network Security and System Software

Curriculum Intent	Pupils will be taught the following National Curriculum guidelines this term:
Skills/Assessment Objective Links	<p><b>At the end of this Unit all students should be able to:</b></p> <ul style="list-style-type: none"> <li>• Understand a variety forms of attack and threats the pose at a basic level</li> <li>• Identify and understand the prevention of vulnerabilities including the use of:               <ul style="list-style-type: none"> <li>– anti-malware software</li> <li>– passwords</li> <li>– physical security</li> </ul> </li> <li>• Explain the need for the following functions of an operating system:               <ul style="list-style-type: none"> <li>– User interface</li> </ul> </li> </ul> <p><b>Most students will be able to:</b></p> <ul style="list-style-type: none"> <li>• Understand forms of attack and threats posed to a network including:               <ul style="list-style-type: none"> <li>– Malware</li> <li>– Phishing</li> <li>– Social engineering</li> <li>– Brute force attacks</li> <li>– Data interception and theft</li> </ul> </li> <li>• Identify and understand the prevention of vulnerabilities including the use of:               <ul style="list-style-type: none"> <li>– penetration testing</li> <li>– user access levels</li> <li>– encryption</li> </ul> </li> <li>• Explain the need for the following functions of an operating system:               <ul style="list-style-type: none"> <li>– User interface</li> <li>– Memory management and multitasking</li> <li>– Peripheral management and drivers</li> <li>– User management</li> <li>– File management</li> </ul> </li> <li>• Describe the purpose and functionality of common utility software including:               <ul style="list-style-type: none"> <li>– Encryption software</li> <li>– Defragmentation software</li> <li>– Data compression software</li> </ul> </li> </ul> <p><b>Some students will be able to:</b></p> <ul style="list-style-type: none"> <li>• Understand forms of attack and threats posed to a network including:               <ul style="list-style-type: none"> <li>• Denial of service attacks</li> <li>• SQL injection</li> </ul> </li> <li>• Identify and understand the prevention of vulnerabilities with the use of firewalls</li> <li>• Explain the need for the following functions of an operating systems including memory management and multitasking</li> </ul>
	<p><b>Numeracy</b>      Data compression</p>
	<p><b>Literacy</b></p> <p><b>Vocabulary Tier 3:</b> Malware, virus, Trojan horse, worm, social engineering, phishing, brute-force attack, denial of service attack, data interception and theft, SQL injection, penetration testing, anti-malware software, anti-virus software, firewalls, user access levels, passwords, encryption, physical security, operating system, user interface, graphical user interface (GUI), command line interface (CLI), memory management, multitasking, peripheral management, drivers, user management, file management, utility software, encryption software, defragmentation, data compression</p> <p><b>Vocabulary Tier 2:</b> File, data, theft, service, attack, user, tests, access, levels</p> <p><b>Reading:</b> Worksheets, presentations, answer sheets, exam questions, mark scheme, further reading for homework</p>

	<p><b>Writing:</b> Answer on the worksheet via word</p> <p><b>Oracy:</b> listening and using tier 3 words</p>
Becoming future ready	<p><b>Careers/Employability:</b></p> <ul style="list-style-type: none"> <li>▪ Software Architect.</li> <li>▪ Data Scientist.</li> <li>▪ Machine Learning Engineer.</li> <li>▪ Blockchain Developer</li> <li>▪ Cybersecurity Engineer.</li> <li>▪ Cloud Solutions Architect.</li> <li>▪ AI Research Scientist.</li> <li>▪ Full-Stack Developer.</li> </ul>
Adaptation	Throughout this topic, quality first teaching will provide differentiation:
QFT/SEND Provision	<p><b>By product:</b> Learners are asked to present outcomes in a different way via pieces of writing, targeted questioning, models and drawings and speaking.</p> <p><b>By resource:</b> Worksheets are well presented and accessible. Instructions are clearly outlined and separate from the information so that pupils know where to begin and end. Handouts are differentiated by outcome. Resources used will appeal to the range of preferred learning styles of pupils e.g. visual, auditory or kinesthetic learners. Scaffolding of tasks – word frames.</p> <p><b>By Intervention:</b> By providing different levels of supervision and support</p> <p><b>By Progressive Questioning:</b> Exploring pupils' understanding through interactive dialogue using Blooms Taxonomy.</p> <p><b>By Grouping:</b> According to prior attainment, gender, social preference, preferred learning style.</p> <p><b>By Task:</b> Pupils identify targets which are meaningful to them via feedback sheets</p> <p><b>By Offering Optional Activities:</b> In class or as homework, to extend learning.</p> <p>This QFT/SEND provision will be explicit within the lesson by lesson schemes of work.</p>
Implementation Curriculum Delivery	To be able to:
Learning Outcomes (Knowledge)	<p><b>Topic 1 Network Threats</b></p> <p>Understand forms of attack and threats posed to a network:</p> <ul style="list-style-type: none"> <li>– Malware</li> <li>– Phishing</li> <li>– Social engineering</li> <li>– Brute force attacks</li> <li>– Denial of service attacks</li> <li>– Data interception and theft</li> <li>– SQL injection</li> </ul> <p><b>Topic 2 Preventing vulnerabilities</b></p> <p>Identify and understand the prevention of vulnerabilities including the use of:</p> <ul style="list-style-type: none"> <li>– penetration testing</li> <li>– anti-malware software</li> <li>– firewalls</li> <li>– user access levels</li> <li>– passwords</li> <li>– encryption</li> <li>– physical security</li> </ul> <p><b>Topic 3 Operating systems</b></p> <p>Explain the need for the following functions of an operating system:</p> <ul style="list-style-type: none"> <li>– User interface</li> <li>– Memory management and multitasking</li> <li>– Peripheral management and drivers</li> <li>– User management</li> <li>– File management</li> </ul> <p><b>Topic 4 Utility software</b></p> <ul style="list-style-type: none"> <li>• Describe the purpose and functionality of common utility software including:</li> </ul>

	<ul style="list-style-type: none"> <li>– Encryption software</li> <li>– Defragmentation software</li> <li>– Data compression software</li> </ul> <p>End of unit assessment</p> 
<b>Current learning to be developed in the future within:</b>	
<b>Assessment</b>	See assessment maps for formative and summative assessment opportunities.
<b>Impact</b>	<p>Review assessment results and target pupils that require further support via:-</p> <ul style="list-style-type: none"> <li>• Learning conversation</li> <li>• Changing seating plan</li> <li>• Plan lessons to address areas of concern in assessment</li> <li>• Targeted homework based on low performance areas identified in the assessment and marked pieces</li> <li>• Stretch and challenge high ability pupils by identifying ambitious next steps to expand knowledge</li> </ul> <p>Create a feedback sheet for each student</p> <p>Each student identifies areas of Green, Amber and Red using Mark Assessment on their feedback sheet</p> <p>Complete NOW task on areas identified as Amber and Red</p>