

CURRICULUM OVERVIEW FOR YEAR 10 COMPONENT 3

EFFECTIVE DIGITAL WORKING PRACTICES

Term	Autumn 1	Autumn 2	Spring 1	Spring 2	Summer 1	Summer 2
Topic	A: Modern technologies A1 Modern technologies A2 Impact of modern technologies	B: Cyber security B1 Threats to data B2 Prevention and management of threats to data	B3 Policy C: The wider implications of digital systems C1 Responsible use C2 Legal and ethical	D: Planning and communication in digital systems D1 Forms of notation	Components A through to C Revision for end of year examination	
Knowledge	Communication technologies Cloud storage Cloud computing Selection of platforms and services Using cloud and traditional systems together Choosing cloud technologies Maintenance, set up and performance considerations Collaborative technologies Using modern technology when managing teams: communication	Why systems are attacked Why systems are attacked External threats to digital systems and data security Internal threats to digital systems and data security User access restriction Data level protection: firewalls and anti-virus software Data level protection: device hardening and encryption Finding weaknesses and improving system security Security policies	Security policies Defining security parameters: passwords Defining security parameters: policies Actions to take after an attack Sharing data The impact of technology on the environment Equal access to information and services Legal requirements and professional guidelines Net neutrality Acceptable use policies Data protection principles	Forms of notation Interpreting data flow diagrams Interpreting flowcharts Interpreting system diagrams Tables and written information Creating data flow diagrams Creating flowcharts	Developing knowledge gained in Terms 1 and 2	

	<p>on and collaboration</p> <p>Using modern technology when managing teams: scheduling and planning</p> <p>Communication with stakeholders</p> <p>Accessibility and inclusivity</p> <p>How modern technologies impact on the organisation</p> <p>How technologies impact the way organisations operate</p> <p>How technology impacts individuals</p>		<p>Data and the use of the internet</p> <p>Intellectual property</p> <p>The criminal use of computer systems</p>			
Skills	<p>Communication technologies: ad-hoc networks, open networks, performance issues and network availability</p> <p>Cloud storage: access rights, synchronisation, availability and scalability</p> <p>"Cloud computing: applications, consistency of versions between users, single</p>	<p>"Why systems are attacked: fun, challenge, espionage, financial gain, personal attack and disruption, theft</p> <p>External threats to digital systems and data: unauthorised access, malware, phishing, pharming, social engineering, shoulder surfing and man-in-the-middle attacks"</p> <p>"Internal threats to</p>	<p>Defining security parameters: passwords and policies</p> <p>"Actions to take after an attack: investigate, respond, manage, recover and analyse</p> <p>Defining security parameters: passwords and policies</p> <p>"Actions to take after an attack: investigate, respond, manage, recover and analyse</p>	<p>Forms of notation: interpreting/creating data flow diagram and flowcharts</p> <p>Forms of notation: interpreting system diagrams, tables and written information</p> <p>"D: assessment practice</p> <p>Revise for final externally-set assessment"</p>		

	<p>shared instances and collaboration tools/features</p> <p>Selection of platforms and services: complexity of features, paid versus free, interface design and available devices"</p> <p>"Using cloud and traditional systems together: device synchronisation, online/offline working and notifications</p> <p>Choosing cloud technologies: disaster recovery policies and security of data"</p> <p>"Maintenance, set up and performance considerations: maintenance: updates, downtime and staff expertise and performance: responsiveness, complexity of task and available devices</p> <p>Collaborative technologies: world teams, multicultural, inclusion, 24/7/365 and flexibility"</p> <p>"Using modern technology when</p>	<p>digital systems and data security: unintentional disclosure of data, intentional stealing or leaking of information, users overriding security controls, portable devices, downloads from the internet and visiting trustworthy websites</p> <p>User access restriction: locks, passwords, levels of permitted access, biometrics and two-factor authentication"</p> <p>Data level protection: firewalls, anti-virus software, device hardening and encryption</p>	<p>B: assessment practice/revision"</p> <p>"Sharing data: benefits, drawbacks and responsible use</p> <p>The impact of technology on the environment: impacts of manufacturing, considerations when upgrading/replacing digital systems and usage of settings policies"</p> <p>"Accessing information and services: benefits to organisations, individuals and society</p> <p>Legal requirements and professional guidelines"</p> <p>"Net neutrality and how this impacts organisations</p> <p>Acceptable use policies: scope, assets, acceptable behaviours, unacceptable behaviours, monitoring, sanctions and agreement"</p> <p>"Data protection principles: lawful processing, specific purposes, relevant data is collected, accuracy, only kept as long as needed, data subject rights</p>			
--	--	---	--	--	--	--

managing teams: communication and collaboration tools
Using technology when managing teams: scheduling and planning tools"
"Communication with stakeholders: communication platforms and selection of appropriate communication channels
Accessibility and inclusivity: interface design, accessibility features and flexibility"
"How modern technologies impact on the organisation: infrastructure, demand, availability, 24/7 access and security of distributed/distributed data
How technologies impact the way organisations operate: inclusivity, accessibility and remote working"
"How technology impacts individuals: flexibility, working styles and impact on

and transferring data to other countries
Data and the use of the internet: right to be forgotten, appropriate legal use of cookies and other transaction data"
"Intellectual property: importance, methods of identifying and legal/ethical use
The criminal use of computer systems: unauthorised access/modification, creation of malware and intentional spreading of malware"

	mental wellbeing A: assessment practice/revisi on"				
Key Marked Piece (Summative Assessments in bold)	Step by Step user guide how to backup and synchronise Presentation on how technology can be used to manage teams	Cybersecurity wiki Report on device hardening techniques	Set of staff guidelines on how to improve password security Case study on organisations and how they defended against cyber attacks	Mock examination Letter to company to advise how to protect against copyright theft	Mock exam prior to final examination Final examination
Vocabulary	Ad-hoc network, network, open network, cloud, synchronisation, access rights, availability, scalability Shared instance, application, collaboration tools, collaboration features, interface design Notifications, cloud technologies, disaster recovery policies, policy, restore Features, online application, version consistency, file sharing Platform, service, interface Traditional system	Attack, digital systems, cyber security, external threat, unauthorised access, malware, phishing, pharming, social engineering, shoulder surfing, man-in-the-middle attacks, potential threat Ransomware, denial of service, wiki Data security, internal threats, override, disclosure, untrustworthy, security breach Prevention, portable device, user access restriction, biometrics, permitted access, two factor authentication Data level protection, firewall, anti-virus, device	Security policy, AUP, disaster recovery policy Security parameters, password policy, usage policy, installation policy, password complexity Software audit Location settings, transactional data, cookies, environmental impacts Legal requirements, professional guidelines WCAG, ethics Open internet code of practice, net neutrality, scope, assets, monitoring, sanctions AUP, social boundaries, business boundaries GDPR, DPA,	Forms, forms of notation, flow chart, processes, digital system Flow diagrams, data flow diagrams, Input, output, process Systems diagrams Numerical data, Data flow diagram	No further vocabulary

	<p>Cloud technology, security, compatibility, maintenance, performance</p> <p>Maintenance, performance, updates, downtime, responsiveness, world teams, multicultural</p> <p>Communication, scheduling, facilitation</p> <p>Collaboration, multiculturalism, inclusivity, flexibility</p> <p>Scheduling, planning</p> <p>Communication channels, private communication, stakeholders, communication platforms</p> <p>Accessibility, inclusivity, interface</p> <p>Infrastructure, distributed data, dispersed data</p> <p>Impact</p> <p>Working style, mental wellbeing</p>	<p>hardening, encryption</p> <p>Security patch</p> <p>Penetration testing, ethical hacking</p>	<p>Transactional data, digital footprint</p> <p>Malware, IP, Trademarks, patents, copyright</p>		
--	---	--	---	--	--