Year 10 & 11 Topics - Tech Award Digital Information Technology

Each topic in Years 10 and 11 develops and deepens the Core knowledge that will underpin all areas of the curriculum at KS4 and KS5. These topics are taught as part of Component 3 : Effective Digital Working Practices.

Component 3: Effective Digital Working Practices

Learning Aim A: Modern technologies				
Topic	**Rationale**	**Knowledge acquisition**	**Key vocabulary**	**Skills and enrichment**
A1 Modern technologies	Students need to understand how and why modern technologies are used by organisations and stakeholders to access and manipulate data, and to provide access to systems and tools in order to complete tasks.	Communication technologies: • setting up ad-hoc networks (open Wi-Fi, tethering/personal hotspot) • security issues with open networks • performance issues with ad hoc networks • issues affecting network availability (rural vs city locations, developed vs developing countries, available infrastructure, mobile network coverage, blackspots)	• Bluetooth • Ad hoc network • Personal area network • Tethering • Open Wi-Fi • Personal hotspot • PIN • Encrypted • USB • Insecure • Streaming • Blackspots	• independence • problem solving • reading • effective writing • oracy • literacy • IT • research • numeracy • communication • working collaboratively • analysis • evaluation • reflective practice
	Students need to understand the implications of these tools and technologies for organisations and stakeholders.	Features and uses of cloud storage: • setting and sharing of access rights • synchronisation of cloud and individual devices • availability (24/7) • scalability (getting more by renting/freeing to save money)	• Server • Downloading • Uploading • Synchronising • Scalability • Cloud storage	
		Features and uses of cloud computing: • online applications • consistency of version between users (features, file types)	• Online applications • Collaboration • File sharing • Live editing	

		• single shared instance of a file • collaboration tools/features		
		How the selection of platforms and services impacts on the use of cloud technologies: • number and complexity of features • paid for versus free • interface design (layout, accessibility, mobile vs desktop) • available devices	• Stakeholders • Downtime • Geo-data • Interface • Platform • Operating system • User interface • RAM • Processing power • Portability • Network connection speed	
		How cloud and 'traditional' systems are used together: • device synchronisation • online/offline working • notifications	• Synchronisation • Online working • Offline working • Remote working • Notifications	
		Implications for organisations when choosing cloud technologies: • consideration of disaster recovery policies (service providers, organisations) • security of data (location, service provider's security procedures and features) • compatibility • maintenance (software updates, downtime, staff expertise) • getting a service/ storage up and running quickly	• Automatic backing up • ISO • PIN • Compatibility • Virtual machines • System administrator • Downtime • Spam • Trash • Dashboard • Cyberattacks • Deploying the device • Operating system • Mail server	

		• performance considerations (responsiveness to user, complexity of task, available devices and communication technologies)	• Incompatibility • Disruption of service	
A2 Impact of modern technologies	Students need to understand how modern technologies impact on the way organisations perform tasks. They should understand how technologies are used to manage teams, to enable stakeholders to access tools and services, and to communicate effectively. They should also understand the positive and negative impact that the use of modern technologies has on organisations and stakeholders.	Changes to modern teams facilitated by modern technologies: • world teams (not bound by geographical restrictions, diversity) • multicultural • inclusivity (facilitation of member's needs) • 24/7/365 (no set work hours, team members in different time zones) • flexibility (remote working vs office based, permanent vs casual staff)	• Collaborative technologies • Conference software • Interoffice chat • Version control • Workflow	• independence • problem solving • reading • effective writing • oracy • literacy • IT • research • numeracy • communication • working collaboratively • analysis • evaluation • reflective practice
		How modern technologies can be used to manage modern teams: • collaboration tools • communication tools • scheduling and planning tools	• Dashboard • Message board • Scheduling • URL – uniform resource locator • File access • Tracking • Timelines	
		How organisations use modern technologies to communicate with stakeholders: • communication platforms (website, social media, email, voice communication) • selection of appropriate communication channels (private/direct message, public status update) for sharing information, data and media	• Website • Social media • Email • Voice communication • Live chat • Private communication • Public communication	

		How modern technologies aid inclusivity and accessibility: • interface design (layout, font and colour selection) • accessibility features (screen reader support, alt text, adjustable typeface/font size, text to speech/’listen to this page’) • flexibility of work hours and locations	• Interface design • Interface layout • Accessibility • ALT text • inclusivity	
		Positive and negative impacts of modern technologies on organisations in terms of: • required infrastructure (communication technologies, devices, local and • web-based platforms) • demand on infrastructure of chosen tools/platforms • availability of infrastructure • 24/7 access • security of distributed/disbursed data • collaboration • inclusivity (age, health, additional needs, multicultural) • accessibility (meeting legal obligations, provision requirements) • remote working	• Infrastructure • Distributed data • Dispersed data • Local platforms • Web based platforms • File sharing • Wikis • Blogs • Chat systems • Video conferencing • Remote working	
		Positive and negative impacts of modern technologies on individuals: • flexibility (home/remote working) • working styles (choice of time, device, location) • impact on individual mental wellbeing (depression, loneliness, self-	• Flexible working • Self-discipline	

		confidence, separation from stressful environment, feel in control of own schedule, schedule adjusted to meet needs of family, less time commuting)		

Learning Aim B: Cyber security				
Topic	**Rationale**	**Knowledge acquisition**	**Key vocabulary**	**Skills and enrichment**
B1 Threats to data	Students need to understand why systems are attacked, the nature of attacks and how they occur, and the potential impact of breaches in security on the organisation and stakeholders.	Why systems are attacked: • fun/challenge • industrial espionage • financial gain • personal attack • disruption • data/information theft	• Intellectual property • Ransomware • Malware • Denial of service attacks • Disruption • Espionage	• independence • problem solving • reading • effective writing • oracy • literacy • IT • research • numeracy • communication • working collaboratively • analysis • evaluation • reflective practice
		External threats (threats outside the organisation) to digital systems and data security: • unauthorised access/hacking (black hat) • malware (virus, worms, botnet, rootkit, Trojan, ransomware, spyware) • denial of service attacks • phishing (emails, texts, phone calls) • pharming • social engineering • shoulder surfing • 'man-in-the-middle' attacks	• Hacking • Black hat • Malware • Virus • Worms • Botnet • Rootkit • Trojan • Ransomware • Spyware • Denial of service attacks • Phishing • Pharming • Social engineering • Shoulder surfing • Man-in-the-middle attacks	

		Internal threats (threats within the organisation) to digital systems and data security: • unintentional disclosure of data • intentional stealing or leaking of information • users overriding security controls • use of portable storage devices • downloads from internet • visiting untrustworthy websites	• Data theft • USB • HTTPS	
		Impact of security breach: • data loss • damage to public image • financial loss • reduction in productivity • downtime • legal action	• Productivity • Public imaged • Downtime	
B2 Prevention and management of threats to data	Students need to understand how different measures can be implemented to protect digital systems. They should understand the purpose of different systems and how their features and functionality protect digital systems. They should also understand how one or more systems or procedures can be	User access restriction: • physical security measures (locks) • passwords • using correct settings and levels of permitted access • biometrics • two-factor authentication (who you are, what you know, what you have)	• Electronic swipe lock • Secured device • CCTV • Permitted access • Biometrics • Two factor authentication	• independence • problem solving • reading • effective writing • oracy • literacy • IT • research • numeracy • communication • working collaboratively • analysis • evaluation • reflective practice
		Data level protection: • firewall (hardware and software) • software/interface design (obscuring data entry, autocomplete, 'stay logged in') • anti-virus software • device hardening	• Firewall • LAN – local area network • ACL - access control list • Obscuring data entry • Autocomplete • Stay logged in	

	used to reduce the nature and/or impact of threats.	- procedures for backing up and recovering data - encryption of stored data (individual files, drive) - encryption of transmitted data	- Worms - Rootkit - Trojan - Spyware - Shoulder surfing - Session cookies - Device hardening - Security patches - Vulnerable - Privilege - Encryption - Algorithm	
		Finding weaknesses and improving system security: - ethical hacking (white hat, grey hat) - penetration testing - analyse system data/behaviours to identify potential risks	- Ethical hacking - Penetration testing - Sytem data - System behaviours - Risk	
B3 Policy	Students need to understand the need for and nature of security policies in organisations. They should understand the content that constitutes a good security policy and how it is communicated to individuals in an organisation. To ensure that potential threats and the impact	Defining responsibilities: - who is responsible for what - how to report concerns - reporting to staff/employees	- System security - Data security - Compliance - Disaster recovery - Data recovery - Infrastructure - Data theft - Virus - Malware	- independence - problem solving - reading - effective writing - oracy - literacy - IT - research - numeracy - communication - working collaboratively - analysis - evaluation - reflective practice
		Defining security parameters: - password policy - acceptable software/installation/ usage policy - parameters for device hardening	- Password strength - Default password - Software audit - Password policy - Usage policy - Parameters	

	of security breaches are minimised, they should understand how procedures in security policies are implemented in organisations.		• Device hardening	
		Disaster recovery policy: • who is responsible for what • dos and don’ts for staff • defining the backup process (what is backed up, scheduling, media) • timeline for data recovery • location alternative provision (hardware, software, personnel)	• Disaster recovery • Timelines • Backup processes • Scheduling • Alternative provision • Hardware • Software	
		Actions to take after an attack: • investigate (establish severity and nature) • respond (inform/update stakeholders and appropriate authorities) • manage (containment, procedures appropriate to nature and severity) • recover (implement disaster recovery plan, remedial action) • analyse (update policy and procedures)	• Stakeholders • GDPR • Data protection controller • Remedial action	

Learning Aim C: The wider implications of digital systems				
Topic	**Rationale**	**Knowledge acquisition**	**Key vocabulary**	**Skills and enrichment**
C1 Responsible use	Students need to consider the responsible use of digital systems, including how systems and services share and exchange data as well as the environmental	Shared data • location-based data • transactional data • Cookies • data exchange between services • benefits of using shared data • drawbacks of using shared data Responsible use • legal considerations	• location-based data • transactional data • cookies • data subject • data exchange • legal responsibility • privacy • ethical	• independence • problem solving • reading • effective writing • oracy • literacy • IT • research • numeracy

	considerations of increased use.	• privacy • ethical use		• communication • working collaboratively • analysis • evaluation • reflective practice
		Environmental: • impact of manufacturing, use, and disposal of it systems (energy, waste, rare materials) • considerations when upgrading or replacing digital systems • usage and settings policies (auto power off, power-saving settings, hard copy vs electronic distribution)	• Consumables • Motherboard • Upgrading • Recycling	
C2 Legal and ethical	Students need to understand the scope and purpose of legislation (valid at time of delivery) that governs the use of digital systems and data, and how it has an impact on the ways in which organisations use and implement digital systems. They should understand the wider ethical considerations of use of technologies, data and information, and organisations' responsibilities to ensure that they	Importance of providing equal access to services and information: • benefits to organisations, individuals and society • legal requirements • professional guidelines/accepted standards	• Email • Online information • Online shopping • E-commerce • Online chat • Media access • Downloads	• independence • problem solving • reading • effective writing • oracy • literacy • IT • research • numeracy • communication • working collaboratively • analysis • evaluation • reflective practice
		Net neutrality and how it impacts on organisations.	• Net neutrality • ISP	
		The purpose and use of acceptable use policies: • scope – who the document applies to • assets – the equipment, documents, and knowledge covered by the policy • acceptable – behaviours that are expected/required by an organisation • unacceptable – behaviours that are not allowed by an organisation	• Discrimination • Race relations • Equality • Offensive content • WCAG – Web content accessibility guidelines • Perceivable • Operable • Understandable • Robust • AUP – Acceptable use policy	

	behave in an ethical manner.	• monitoring – description of how behaviour is monitored by an organisation • sanctions – defining the processes and potential sanctions if unacceptable • behaviour occurs • agreement – acknowledge (sign, click) that an individual agrees to abide by the policy		
		Blurring of social and business boundaries: • use of social media for business purposes • impact of personal use of digital systems (social media, web) on professional life	• Third party cookies • Vlogger • Blogger • Social media	
		Data protection principles: • lawful processing • collected only for specific purpose • only needed information is collected • should be accurate • kept only as long as is necessary • data subject rights • protected • not transferred to countries with less protection	• Data protection • GDPR • Lawful processing • Accuracy • Data subject rights	
		Data and the use of the internet: • the right to be forgotten • appropriate and legal use of cookies and other transactional data	• Digital footprint • Cookies • Right to be forgotten • Ethical constraint • Tracking cookie • Transactional data • E-privacy directive	

		Dealing with intellectual property: • the importance of intellectual property in organisations • methods of identifying/protecting intellectual property (trademarks, patents copyright) • legal and ethical use of intellectual property (permissions, licensing, attribution)	• Patent • Trademark • Brand • Copyright • Plagiarism • Intellectual property	
		The criminal use of computer systems: • unauthorised access • unauthorised modification of materials • creation of malware • intentional spreading of malware	• Peer to peer (P2P) • Cracks • Malware • Encryption	

Learning Aim D: Planning and communication in digital systems				
Topic	**Rationale**	**Knowledge acquisition**	**Key vocabulary**	**Skills and enrichment**
D1 Forms of notation	Students need to able to interpret and use standard conventions to combine diagrammatical and written information to express an understanding of concepts.	Understand how organisations use different forms of notation to explain systems, data and information: • data flow diagrams • flowcharts • system diagrams • tables • written information	• Notation • Information flow diagram • Database • Hardware • Software • Component • Data flow diagram	• independence • problem solving • reading • effective writing • oracy • literacy • IT • research • numeracy • communication • working collaboratively • analysis • evaluation • reflective practice
		Be able to interpret information presented using different forms of notation in a range of contexts.	• Notation	
		Be able to present knowledge and understanding using different forms of notations: • data flow diagrams	• Data flow diagram • Information flow diagram • Flowchart • Date store	

		• information flow diagrams • flowcharts	• Entity • Terminator • Process • Decision • Data • Output	