Share Multi Academy Trust

Subject:	BTEC DIT	Year	11 2023/24	Ability	Mixed

Component 3: Effective digital working practices Learning Aim A: Modern Technologies **Learning Aim B**: Cyber Security **Learning Aim C**: The wider implications of digital systems **Learning Aim D**: Planning and communication in digital systems.

Terms	**A1: HT4**	**A2: HT4**	**B1: HT4**	**B2: HT4**	**B3:HT5**	**C1: HT5**	**C2: HT6**	**D1: HT6**
Topic	**Component 3: A1 Modern Technologies** Learning Aim, A: Modern Technologies	**Component 3: A2 Impact of modern technologies** Learning Aim, A: Modern Technologies	**Component 3: B1 Threats to data** Learning Aim B: Cyber Security	**Component 3: B2 Prevention and management of threats to data** Learning Aim B: Cyber Security	**Component 3: B3 Policy** Learning Aim B: Cyber Security	**Component 3: C1: Responsible use** Learning Aim C: The wider implications of digital systems	**Component 3: C2: Legal and ethical** Learning Aim C: The wider implications of digital systems	**Component 3: D1 Forms of notation** Learning Aim D: Planning and communication in digital systems
Topic overview **Students will learn…**	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.	How modern technologies impact organisations and individuals, are used to manage teams, communicate with stakeholders and aid accessibility	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.	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.	About security policies in organisations. They will learn about the content that constitutes a good security policy and how it is communicated to individuals in an organisation.	The responsible use of digital systems, including how systems and services share and exchange data as well as the environmental considerations of increased use.	The scope and purpose of legislation 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. Students will also learn the wider ethical considerations of the use of technology, data and information.	How to interpret and use standard conventions to combine diagrammatical and written information to express an understanding of concepts.
Components	Students will learn about communication technologies in order to understand how essential these are to both business and personal lives. This will cover: • Setting up ad-hoc networks • Security issues with open networks • Performance issues with ad-hoc networks • Issues affecting network availability • menus and forms. Students will learn the features and uses of	Students will learn about the changes technology has made to modern teams in order to collaborate, communicate and plan together. They will learn about • Worldwide and multicultural teams • Workplace inclusivity • Changing work schedules • Flexible work locations Students will learn how modern technologies have changes the way	Students will learn why systems are attacked and the impact security breaches have on organisations in order to understand why systems are targeted. Reasons why systems are attacked include: • Fun/challenge • Industrial espionage or financial gain • Personal attack • disruption • data/information theft Impact of security breach:	Students will learn how different measures can be implemented to protect digital systems in order to find procedures that can reduce the impact of threats. These will include: • **User access restriction**: physical security, passwords, using correct settings and levels of permitted use, biometrics, two-factor authentication (who you are, what	Students need to understand the need for and nature of security policies in order to protect organisations from the impacts of a cyber security incident, They need to know how procedures in security policies are implemented in order to minimise the potential threat and impact of a security breach: To do this they will learn about: • **Defining responsibilities:** who is responsible	Students will learn about the use of shared data in order to understand the ethical and legal responsibility we have when handling data. This includes: • Collecting and sharing data • The benefits and drawbacks of shared data • The importance of responsible use of shared data. Students will also learn about the environmental concerns in order to understand the impact technology	Students will learn about the importance of providing equal access to services and information in order to understand the digital divide and the laws preventing this. They will look at: • **Equal access and net neutrality**: The benefits to organisations, individuals and society of equal access, the legal requirements, professional guidelines/professional standards	Students will learn how organisations use different forms of notation in order to explain systems, data and information. This will include: • Data flow diagrams • flowcharts • system diagrams • tables • written information Students will also learn how to interpret and present information using different forms of notation in order to understand which notation is suitable for

	cloud storage and cloud computing in order to assess their use in both personal and professional lives. This will include: • Setting and sharing access rights • Synchronisation of cloud and individual devices • Availability • Scalability • Online applications • Consistency of version between users • Single shared instance of a file • Collaboration tools and features Students will learn about choosing a cloud service in order to understand when to use cloud computing and when to use traditional computing: They will learn about: • Number and complexity of features • Paid vs Free • Interface design • Available devices • Device synchronisation • Online / offline working • Notifications Students learn about the factors that have to be considered in choosing a cloud service in order to understand the implications of cloud technologies.	we manage teams in order to understand the different tools that can be used to support collaboration, communication and scheduling and planning. Students will learn how modern technologies can be used to communicate with stakeholders and aid inclusivity and accessibility in order to understand the impact this has on modern working methods. This will include: • Communication platforms • Public and private communication channels • Interface design • Accessibility features • Flexibility of work hours and location. Students next learn about the impact of modern technology on organisations in order to understand how modern technologies have changed the way businesses are organised. This will include: • The impact on infrastructure demands, availability and security • The impact on operation: collaboration, inclusivity and accessibility, remote working.	• Data loss • Damage to public image • Financial loss • Reduction in productivity • Downtime • Legal action Threats to systems are broken down into internal and external threats. Students will learn about the different types of threats in order to understand how to prevent and mange threats. External threats: • Social engineering threats such as phishing and shoulder surfing • Malware threats such as virus, worms, botnet, rootkit, trojan, ransomware, spyware • Hacking (black hat) • Pharming • Man-in-the-middle attacks Internal threats: • Unintentional disclosure of data • Intentional stealing or leaking of information • Users overriding security controls • Use of portable storage devices • Downloads from internet	you are, what you have) • **Data level protection**: firewall (hardware and software), software/interface design, Anti-virus software, Device hardening, Procedures for backing up and recovering, Encryption of stored data, Encryption of transmitted data • **Finding weaknesses and improving system security**: ethical hacking (white hat, grey hat), penetration testing, analyse system data/behaviours to identify potential risks.	for what, how to report concerns, reporting to staff/employees • **Defining security parameters**: password policy, acceptable software/installation/usage policy, parameters for device hardening • **Disaster recovery policy**: who is responsible for what, dos and don'ts for staff, defining the backup process, timeline for data recovery, location of alternative provision • **Actions to take after an attack**: Investigate, respond, manage, recover, analyse	has on the environment This will include: • The impact of the manufacturing, use and disposal of IT systems • The consideration when upgrading or replacing digital systems • Usage and settings policies that effect the environment.	• **The purpose and use of Acceptable use policies:** scope, assets, acceptable, unacceptable, monitoring, sanctions, agreement • **Social and business boundaries:** use of social media for business, personal use of digital systems in work life • **Data protection principles** • **Data and the use of the Internet:** the right to be forgotten, cookies and other transactional data • **Dealing with intellectual properties:** identifying and protecting intellectual property, law and ethics • **Criminal use of computer systems:** unauthorised access, unauthorised modification of materials, creation of malware, intentional spreading of malware Students will also learn different ways to use design software in order to create their own designs	a certain type of information. .

	This will include: • Consideration of disaster recovery policies • Security of data • Compatibility • Maintenance • Getting a service/software up and running • Performance considerations	Finally, students learn about the impact of modern technology on individuals in order to understand how modern technologies have affected our personal and working lives. This will include: • Flexibility • Working styles • Mental well being	• Visiting untrustworthy websites.					
What students should already know (prior learning components)	Students have covered the following at KS3: Understand the hardware and software components that make up a computer system and how they communicate with one another and with other systems This is covered in Year 7: Computer parts and logic gates and Graphics programming and in Year 8: How computer's work and Graphics and Gaming	Students should have covered Component 3: A1, the previous topic, as they need a knowledge of cloud storage, cloud computing, different devices and synchronisation. Also, the same KS3 component as A1	Students have covered the following at KS3: Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy, recognising inappropriate content, contact and how to report concerns. This is covered in the Yr. 9 Cyber security unit.	Students need to have completed the previous topic on threats to data so they can look at how to prevent such threats. Also, the same KS3 component as B1	Students need to have completed the previous topics on threats to data and prevention and management of threats so they can look at how policy is created and understand what actions need to be taken after an attack.	Students have covered the following at KS3: Understand the hardware and software components that make up a computer system and how they communicate with one another and with other systems This is covered in Year 7: Computer parts and logic gates and Graphics programming and in Year 8: How computer's work and Graphics and Gaming Understand a range of ways to use technology safely, respectfully, responsibly and securely. This is covered in the Yr. 9 Cyber security unit Design, use and evaluate computational abstractions that model the state and behaviour or real-world problems and physical systems This is covered in the Yr. 9 unit on Data Science.	Students have covered the following at KS3: Understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and privacy, recognising inappropriate content, contact and how to report concerns. This is covered in the Yr. 9 Cyber security unit Completion of the previous topic.	This is a new topic so no prior knowledge is required though the use of tables and charts is used in Yr. 7 spreadsheets, Yr. 8 data handling and Yr. 9 Data Science

Transferrable knowledge (skills)	The setting up of ad-hoc networks; how cloud storage and cloud computing are used; how to synchronise devices; using Bluetooth; using collaboration tools; using notifications.	Using remote working and how to work as part of an international modern team; mental wellbeing; online and offline working.	External and internal threats to your personal data including being hacked, social engineering and the use of malware.	How to prevent cyber attacks both in an organisation and on personal devices. Knowing how to create a secure password and use physical security measures. How to use biometrics and two-factor authentication	Creating policies that ensure compliance with laws and regulations and being able to follow a disaster recovery policy.	Knowing how to share data responsibly. Understand the impact of technology on the environment.	Know about equal access policies, the digital divide and net neutrality. Understand the principles of the Data protection act as they apply to you. Know about intellectual property involving patents, trademarks and copyright.	How to create flowcharts, system diagrams and data flow diagrams. How and when to use tables and charts to present data.
Key vocabulary pupil will know and learn	Personal Area Network (PAN), tethering, Bluetooth, personal hotspot, PIN, encrypted, USB, insecure, streaming, ad-hoc, blackspots, cloud storage, cloud computing, synchronising, uploading, downloading, server, stakeholders, downtime, geo-data, spam, version control	Collaboration, URL, stakeholders, ALT Text, accessibility, inclusivity, interface, 27/7, Wiki, blogs, wellbeing.	Intellectual property, ransomware, malware, Denial of service attack, Social engineering, phishing, hacking, pharming, man-in-the-middle, productivity, shoulder surfing, worms, trojans, rootkits, spyware	Swipe card, biometrics, two-factor authentication, firewall, Local area network (LAN), Wide area network (WAN), Access control list, session cookies, device hardening, vulnerable, security patches, privilege, encryption, ethical hacking, penetration testing, default password, software audit, data protection controller, remedial action	Default password, software audit, data protection controller, remedial action	GPS, transactional data, data subject, consumables, motherboard, upgrading, discrimination	Net neutrality, third party cookies, capturing data, processing data, digital footprint, trademark, patent, copyright, plagiarism, peer to peer, cracks	Notation, information flow diagram, data flow diagram, flow charts, executive summary
Assessment activities	**Formative** –verbal assessment through in class questioning and discussion. Recall activities through class discussion and completion of in-class worksheets Completion of homework units designed to apply their knowledge in real-life situations and check understanding. Homework 1 will be given at the completion of Topic 1 LAA MS Teams	**Formative - as for A1** LAA MS Teams Topic 2 – Impact Homework Quizzes **Summative** This assessment will cover the topics taught so far. The questions will be a mixture of short answer, matching and exam style questions. (40 marks) The exam style questions will focus on those areas also covered in the exam component, namely, audience needs, accessibility and design features.	**Formative - as for Section A** LAB MS Teams Topic 1 – Threats to Data Homework Quizzes	**Formative - as for Section A** LAB MS Teams Topic 2 – Prevention Homework Quizzes	**Formative - as for Section A** LAB MS Teams Topic 3 – Policy Homework Quizzes **Summative** This assessment will cover the topics taught so far. The questions will be a mixture of short answer, matching and exam style questions. (40 marks) The exam style questions will focus on those areas also covered in the exam component, namely, audience needs,	**Formative - as for Section A** LAC MS Teams Topic 1 – Responsible Use Homework Quizzes	**Formative - as for Section A** LAC MS Teams Topic 2 – legal & Ethical Homework Quizzes **Summative** This assessment will cover the topics taught so far. The questions will be a mixture of short answer, matching and exam style questions. (40 marks) The exam style questions will focus on those areas also covered in the exam component, namely, audience needs,	**Formative - as for Section A** LAD MS Teams Topic 1 – Forms of Notation Homework Quizzes **As all content has now been complete, students will be regularly completing recall activities and exam style questions** **Summative** Terminal exam

	Topic 1 – Modern Technologies Homework Quizzes				accessibility and design features.		accessibility and design features.	
Resources available	Pearson Student Textbook Pearson Student Resources on Ms Teams 1 - Modern technologies LAA	Pearson Student Textbook Pearson Student Resources on Ms Teams 2- Impact LAA	Pearson Student Textbook Pearson Student Resources on Ms Teams 1 - Threats to data LAB	Pearson Student Textbook Pearson Student Resources on Ms Teams 2- Prevention LAB	Pearson Student Textbook Pearson Student Resources on Ms Teams 3 - Policy LAB	Pearson Student Textbook Pearson Student Resources on Ms Teams Topic 1 - Responsible use LAC	Pearson Student Textbook Pearson Student Resources on Ms Teams Topic 2 - Legal and ethical LAC	Pearson Student Textbook Pearson Student Resources on Ms Teams Topic 1 - Forms of notation LAD
Notes **Why this topic is important…**	Students need to know about how modern technologies are used by, and have an impact on, organisations and their stake holders to exchange information, communicate and complete work related tasks. This knowledge is the basis of the forthcoming units but also essential knowledge in the modern world as it affects both our business and personal lives.	Following on from the previous topic, students now need to understand how modern technologies impact on the way organisation perform tasks, whether positively or negatively. It is important to know how technology is used to manage teams, enable stakeholders to access tools and services, and to communicate effectively as this will be used in subsequent topics but also in every day working and personal life.	Organisations use digital systems every day to carry out tasks, store data, and manage operations vital to the company. For students to have an understanding of why systems are the targets of attacks and the implications of these attacks, students must first learn some of the most popular types and impacts of cyber threats.	In order to ensure that a system is secure, businesses will put in place physical and software-based prevention methods. Students need to understand the purpose of different measures and how their functions and functionality protect digital systems in order to know which measures to use and why.	Organisations implement policies and procedures as a road map for day-to-day operations. They are extremely important in making sure a business complies with laws and regulations and employees know their responsibilities. Students need to understand need to understand the nature of these security policies, what makes a good one and how the polices are implemented.	Data is the driving force of businesses in today's modern society. Companies use the data they acquire to provide services, tailor products and personalise adverts. It is therefore important that this data is handled responsibly and this topic explains how this is done and what the benefits and drawbacks are of sharing data. Devices are an essential part of most of our lives, and help us to complete daily tasks. However, these devices can have a negative impact on the environment. Students need to understand the wider implications of using digital systems and devices.	One of the biggest ethical issues with IT in modern society is unequal access to devices and the Internet. Students will learn about equal access and net neutrality as ways to avoid this. Another important ethical issue is how technology has affected our work/life balance and this is another area students will study. In the previous topic students looked at the importance of protecting data. Students now learn about the data protection Act and the principles of the act that govern the use of data. Finally, two of the biggest ethical issues connected with IT systems are copyright infringement and computer crime. Students will learn about the laws	When planning a solution, whether it is a hardware solution or a software one, we need ways to communicate this plan to individuals. There are several different methods of communicating this information and students need to know when to use what method and why otherwise plans and solutions will not be communicated clearly.

							governing these issues but will also learn how hard they are to enforce.	