Meden School Curriculum Planning							
Subject	BTEC DIT	Year Group	11	Sequence No.	MTP 6	Topic	Component 3 Learning aim B

Retrieval	Core Knowledge	Student Thinking
What do teachers need retrieve from students before they start teaching new content?	What specific ambitious knowledge do teachers need teach students in this sequence of learning?	What real life examples can be applied to this sequence of learning to development of our students thinking, encouraging them to see the inequalities around them and 'do something about them!'
In ICT / CS at Meden in KS3, pupils are taught to: • design, use and evaluate computational abstractions that model the state and behaviour of real-world problems and physical systems • undertake creative projects that involve selecting, using, and combining multiple applications, preferably across a range of devices, to achieve challenging goals, including collecting and analysing data and meeting the needs of known users • create, reuse, revise and repurpose digital artefacts for a given audience, with attention to trustworthiness, design and usability • understand a range of ways to use technology safely, respectfully, responsibly and securely, including protecting their online identity and	This component will give students an opportunity to explore how the developments in technology over recent years have enabled modern organisations to communicate and collaborate more effectively than ever before. The component is designed to allow students to explore the digital systems available to organisations and how their features have an impact on the way organisations operate. Students will explore how developments in technology have led to more inclusive and flexible working environments, and how regulation and ethical and security concerns influence the way in which organisations operate. Students will analyse information in a range of vocational contexts so that students develop a greater understanding of the use of digital systems by organisations and so that students are able to make reasoned judgements on the systems. In this component, students will learn about how organisations can use technology safely and about the cyber security issues when working in a digital organisation. Learning aim B: Cyber security Learners must understand how the increased reliance of organisations on digital systems to hold data and perform vital functions presents a range of challenges and dangers. They should understand the nature of threats to digital systems and ways that they can be mitigated through organisation policy, procedures and the actions of individuals. They should be able to apply knowledge of cyber security to a range of vocational contexts.	Searching and applying for jobs in ICT, IT and computing. Be able to plan a project and create smart goals and objectives. Students will be able to use spreadsheet software to design and analyse data. To create charts to analyse data.

privacy; recognise inappropriate content, contact and conduct, and know how to report concerns	B1 Threats to data Learners should 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: o fun/challenge o industrial espionage or financial gain o personal attack o disruption o data/information theft. ● External threats (threats outside the organisation) to digital systems and data security: o unauthorised access/hacking (black hat) o malware (virus, worms, botnet, rootkit, Trojan, ransomware, spyware) o denial of service attacks or phishing (emails, texts, phone calls) o pharming o social engineering o shoulder surfing o 'man-in-the-middle' attacks. ● Internal threats (threats within the organisation) to digital systems and data security: o unintentional disclosure of data o intentional stealing or leaking of information o users overriding security controls o use of portable storage devices o downloads from internet o visiting untrustworthy websites. ● Impact of security breach: o data loss o damage to public image o financial loss o reduction in productivity o downtime	

	o legal action. B2 Prevention and management of threats to data Learners should 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. Learners should understand how one or more systems or procedures can be used to reduce the nature and/or impact of threats. ● User access restriction: o physical security measures (locks) o passwords o using correct settings and levels of permitted access o biometrics o two-factor authentication (who you are, what you know, what you have). ● Data level protection: o firewall (hardware and software) o software/interface design (obscuring data entry, autocomplete, 'stay logged in') o anti-virus software o device hardening o procedures for backing up and recovering data o encryption of stored data (individual files, drive) o encryption of transmitted data. ● Finding weaknesses and improving system security: o ethical hacking (white hat, grey hat) o penetration testing o analyse system data/behaviours to identify potential risks. B3 Policy Learners should 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 of security	

	breaches are minimised, learners should understand how procedures in security policies are implemented in organisations. ● Defining responsibilities: o who is responsible for what o how to report concerns o reporting to staff/employees. ● Defining security parameters: o password policy o acceptable software/installation/usage policy o parameters for device hardening. ● Disaster recovery policy: o who is responsible for what o dos and don'ts for staff o defining the backup process (what is backed up, scheduling, media) o timeline for data recovery o location alternative provision (hardware, software, personnel). ● Actions to take after an attack: o investigate (establish severity and nature) o respond (inform/update stakeholders and appropriate authorities) o manage (containment, procedures appropriate to nature and severity) o recover (implement disaster recovery plan, remedial action) o analyse (update policy and procedures).	
Vocab List: Hacker, system attack, black hat, white hat, grey hat, malware, virus, worm, botnet, rootkit, Trojan, ransomware, spyware, Denial of Service, phishing, pharming, social engineering, shoulder surfing, 'man-in-the-middle' attacks, unintentional disclosure, information theft, security controls, security breach, internal threat, passwords, access levels, biometrics, two-factor authentication, ethical hacking, penetration testing, system analysis, behaviour analysis, firewall, interface design, autocomplete, anti-virus, device hardening, encryption, cyber security, policy, acceptable use policy (AUP), disaster recovery, backups		