Long-term planning

Digital Information Technology - Year 11

Year 11	Autumn term 1	Autumn term 2	Spring term 1	Spring term 2	Summer term 1	Summer term 2
	Students will know that	**Students will know that**	**Students will know that**	**Students will know that**	**Students will know that**	**Students will know that**
	Global Positioning System (GPS) is a navigational system that uses data transmitted by satellites to calculate the location of the GPS-enabled device. Every single day organisations generate, process and store large amounts of data using a range of technologies. Organisations must think about how data is used and shared to ensure data is manged lawfully. Location-based services contribute to fraud-prevention as your location can be matched with the place your bank or credit card is used. Transactional data is generated when purchasing things. A cookie is a text file carrying some information that a website places on a user's computer. Cookie data is used by organisations to tailor user experience and target advertisements. Shared data is beneficial as more information means better decisions, however it should be done so in a legal and ethical way, maintaining privacy.	Unauthorised access is where users attempt to gain access to remote systems without the permission or authorisation of their owners to do so legally. This type of behaviour is referred to as “black hat” hacking. Hacking that is legally performed by paid specialists testing the security of digital systems is called “white hat” or ethical hacking. Social engineering is manipulating people into handing over confidential information such as a PIN or password through shouldering and phishing. Malware is malicious software intentionally designed to cause harm. Different types of malware include: virus, worm, trojan, botnet, rootkit, ransomware, spyware. Phishing is a cyberattack that sends spam messages to try and trick people to reply with desired information. Pharming is a cyberattack that uses malware to direct a user to	Security policies are created to ensure that all employees in all locations have a set of responsibilities and procedures to follow when using IT systems. Examples of security policies include: system security, data security, compliance, environmental, disaster recovery, data recovery, infrastructure and responsible use policies. Policies exist to increase the robustness of IT systems and data and to plan for what should happen in the event of a disaster. E.g. virus/theft of data/data loss etc. Password policies are put in place to ensure that during the creation of passwords the passwords individuals create are forced to be more complex. Default passwords are automatically allocated when your account is set up. Users are always advised to change default passwords on first use. Acceptable software policies are used to ensure users do not install any software that may contain malware or suspicious content.	(Revision for component 3 – Examination potentially in the first week/second week in 2027)	(Revision for component 3 – Examination potentially in the first week/second week in 2027)	XXX

	Technology use impacts the environment such as using non-renewable resources, energy consumption and the disposal of e-waste. Users can do things such as powering off devices, using power saving mode and limiting printing of documents to reduce the impact their technology usage is having on the environment. Some countries illegally send their e-waste to third world countries. People in these countries are exposed to toxic substances when trying to extract the metals. The benefits to organisations, individuals and society are faster communication, greater convenience, wider access to information/files/documents. Organisations must work within a legal framework that covers their use of digital technologies, data and information. Web Accessibility Initiative (WAI) is a family of standards that include 4 principles of Web Content Accessibility Guidelines (WCAG) – Perceivable, Operable, Understandable, Robust. Net neutrality is the principle that internet service providers should enable access to all content and applications regardless of the source, and without favouring or blocking particular products or websites.	a fake website that requests information. Internal threats can happen via visiting untrusted websites, allowing the use of portable storage devices, downloading files off the internet, disclosure of data, stealing or leaking information or users overriding security controls. Physical security techniques are used to act as a deterrent and to stop attackers from gaining direct and physical access to locations where data is store e.g. electronic swipe card, secured device, CCTV. Authentication checks to see if a correct user input matches expected input by doing comparison checks. A firewall helps to protect a network by monitoring incoming and outgoing traffic and using a set of rule to determine which traffic to allow in and out. Access control list (ACL) is a list that tells the network which data can be sent and received. Anti-malware has three purposes: • To detect malware that has been installed • To prevent malware from being installed	A software audit is a manual or automated process that lists the name, version and installation date of all software found on a digital device. When an attack has happened on an organisation they should follow the steps of: investigate, respond, manage, recover and analyse. A Data Protection Controller is the named person in an organisation who takers responsibility for the safety and security of the organisation's data. Remedial action is an action taken to fix something that has gone wrong; a remedy. Longer-term remedial action may include changes to policy, procedures, investments in new hardware and/or software, increase device hardening or better employee education and training.			

	General Data Protection Regulation (GDPR) is a European-wide law that tightens data privacy and gives data subjects extra rights, including things such as the right to be informed, the right of access and the right to object. Intellectual property refers to the creations of the human intellect and copyright, patents and trademarks help protect them. Trademark is the recognisable design, words or symbols that have been legally registered by a company or individual for a company, product or name. Patent is the exclusive rights granted to a person or organisation for a specific idea, design or invention. Copyright is a legal right protecting the use of your work. There are different rules about how and why your work could ne used and how long copyright is retained. Plagiarism is copying someone else's work or intellectual property without acknowledging them, claiming it as your own. Using content without permission or acknowledgment could lead to, being asked to stop, taken court or paying a fine/compensation. There are 4 main areas of common criminal use of	• To remove malware from the system Encryption is the scrambling of files and data so that they cannot be read if they are accessed by an attacker. It is common practice to encrypt data when it is stored and when it is being transmitted between IT systems. Ethical hacking is a process where an individual or a team of penetration testers are asked by an organisation to simulate an attack on its IT system to highlight any weaknesses or vulnerabilities. Ethical hackers can be described as white-hat hackers or grey-hat hackers. Penetration testing is the systematic process used by ethical hackers to determine the security of an IT system. It can be an expensive process.				

	computer systems: unauthorised access, unauthorised modification of materials, creation of malware, intentional spreading of malware. A peer-to-peer (P2P) is a way of sharing information or data with other people without the need of a central server. An illegal P2P network downloads of copyrighted material is a common way of spreading malware. Notation means using symbols to represent something. In IT this means using diagrams to represent a range of ideas. An information flow diagram is a diagram that shows how information flows around a system. It is just about the different components of information that a system handle. Data flow diagrams are made up of four key components. Different versions of these diagrams may use slightly different symbols, but the meaning will still be the same. The flowchart symbols: start/end, process, input/output, decision and sub are used to create a diagrammatic representation of an algorithm.					

	Students will know how	Students will know how	Students will know how	Students will know how	Students will know how	Students will know how
	To describe the advantages and disadvantages of shared data. To discuss the impact of the manufacturing, use and disposal of IT systems. To identify considerations when upgrading or replacing digital systems. To explain principles of the Data Protection Act and GDPR that businesses and individuals must follow to be compliant with these legislations. To identify the impact of an organisation not being compliant with legislations. To represent a range of notation diagrams e.g. information flow diagrams, data flow diagrams, system diagrams and flowcharts.	To identify the different types of malware based on their characteristics. To describe the different ways a security breach can impact an organisation such as: data loss, damage to public image, financial loss, downtime, reduction in productivity, legal actions. To identify different ways of authenticating a user. E.g. multi-factor authentication, biometrics To explain benefits and drawbacks of encryption, including its importance when transmitting data. To describe the difference between white-hat hackers and grey-hat hackers. To explain reasons why organisations might use ethical hackers. To evaluate previous practical work completed and know how to make improvements based on teacher feedback. To complete a project proposal, plan timescales, design an initial user interface of four screens and develop a working prototype. To select appropriate project planning tools that are suitable for the project brief given.	To describe different types of policies used by organisations. To identify what should be included in a disaster recovery plan. To identify features of password strength. To identify external threats that often request users to update passwords. To explain why default passwords should be changed. To identify the risks of installing and using unapproved software. To describe how an acceptable software policy might be enforced. To describe what a software audit is. To describe the actions carried out by an organisation after an attack.	To evaluate previous practical work completed and know how to make improvements based on teacher feedback. To create a professional looking dashboard that presents data in an easy to read and understand format. It should allow the user to draw meaningful and accurate conclusions from the information presented. To identify gaps in their own knowledge to target revision to these areas. To apply revision strategies to Digital Information Technology for Component 3.	To reflect on progress made in year 10 and 11. To identify gaps in their own knowledge to target revision to these areas. To apply revision strategies to Digital Information Technology for Component 3.	XXX

		To create a user interface that takes into account all the project planning techniques learnt. To constructively review a user interface that takes into account all the project planning techniques learnt. To make suggestions that could improve the user interface.				
	Vocabulary and the concepts they link to	**Vocabulary and the concepts they link to**	**Vocabulary and the concepts they link to**	**Vocabulary and the concepts they link to**	**Vocabulary and the concepts they link to**	**Vocabulary and the concepts they link to**
	GPS, Location-based services, Data, Information, Fraud, Transactional Data, Data Protection Act, Cookie, Advertisements, Non-Renewable, Energy Consumption, Recycling, Disposal, E-Waste, Discrimination, Web Accessibility Initiative (WAI), Web Content Accessibility Guidelines (WCAG), Net Neutrality, Internet Service Provider (ISP), Applications, Website, Social Media, General Data Protection Regulation (GDPR), Intellectual Property, Trademark, Patent, Copyright, Plagiarism, Licensing, Content, Malware, Computer Misuse Act, Peer-to-peer	Social engineering, Phishing, Pharming, Ethical hacking, White-hat hacking, Grey-Hat hacking, Penetration Testing, Malware, Virus, Worm, Trojan, Botnet, Rootkit, Ransomware, Spyware, Authentication, Firewall, Access control list (ACL), Encryption	Policy, Passwords, Security Policies, Default passwords, Acceptable software policies, software audit, Data Protection Controller, Remedial action, Hardware, Software		(Revision for component 3)	XXX
	Assessment	**Assessment**	**Assessment**	**Assessment**	**Assessment**	**Assessment**
	Component 3 assessment (A/C/D) Low stakes quizzes	PSA Low stakes quizzes	Component 3 assessment (FULL) Low stakes quizzes	PSA Low stakes quizzes	Final BTEC examination (Externally assessed)	XXX
	Diversity & development of cultural capital	**Diversity & development of cultural capital**	**Diversity & development of cultural capital**	**Diversity & development of cultural capital**	**Diversity & development of cultural capital**	**Diversity & development of cultural capital**
	Spiritual – use of imagination and creativity and reflective of their experiences	Spiritual – use of imagination and creativity and reflective of their experiences	Spiritual – use of imagination and creativity and reflective of their experiences	Spiritual – use of imagination and creativity and reflective of their experiences	Spiritual – use of imagination and creativity and reflective of their experiences	XXX

	Moral – Accessibility Moral – Computer Misuse Act Moral – Computer Science professionalism in coding careers Moral - E-waste is often shipped abroad to countries with a lower standard of disposal Moral – What does your household do with old electronic devices that are no longer used? Social – class/group discussions	Moral – Computer Misuse Act Moral – Computer Science professionalism in ethical hacking Social – class/group discussions	Moral – Computer Misuse Act Moral – Abiding by user policies Moral – Complex passwords vs basic passwords Social – class/group discussions	Social – class/group discussions	Social – class/group discussions	
	Cross-curricular opportunities and enrichment	**Cross-curricular opportunities and enrichment**	**Cross-curricular opportunities and enrichment**	**Cross-curricular opportunities and enrichment**	**Cross-curricular opportunities and enrichment**	**Cross-curricular opportunities and enrichment**
	Science - Fossil fuels Geography – Third world countries (e-waste) Business Studies – How businesses use technology	Business Studies – planning a project Design and Technology – Design principles, prototyping. Art – colour schemes, proportion, placement Computer Science – Ethical Hacking/Penetration Testing	Safer Internet Day	National Careers Week Computer Science – Data and information. Sorting. Business Studies – using, displaying and interpreting data.		XXX