




## BTEC Pearson Digital Information Technology – Component 3 Exam

				Revision material Created	Exam Question Answered
Learning Aim A: Modern Technologies					
Learning Aim A: A1 – Modern Technologies					
Communication Technologies <ul style="list-style-type: none"> <li>• Setting Up ad hoc networks</li> <li>• Security issues with open networks</li> <li>• Performance issues with ad hoc networks</li> <li>• Issues affecting network availability</li> </ul>					
Features and uses of Cloud storage <ul style="list-style-type: none"> <li>• Setting and sharing access rights</li> <li>• Synchronization of cloud and individual devices</li> <li>• Availability (24/7)</li> <li>• Scalability</li> </ul>					
Features and uses of cloud computing: <ul style="list-style-type: none"> <li>• online applications</li> <li>• consistency of version between users (features, file types)</li> <li>• single shared instance of a file</li> <li>• collaboration tools/features.</li> </ul>					
How the selection of platforms and services impacts on the use of cloud technologies: <ul style="list-style-type: none"> <li>• number and complexity of features</li> <li>• paid for versus free</li> <li>• Interface design (layout, accessibility, mobile versus desktop)</li> <li>• available devices.</li> </ul>					
How cloud and 'traditional' systems are used together: <ul style="list-style-type: none"> <li>• device synchronisation</li> <li>• online/offline working</li> <li>• notifications.</li> </ul>					
Implications for organisations when choosing cloud technologies: <ul style="list-style-type: none"> <li>• consideration of disaster recovery policies</li> <li>• security of data</li> <li>• compatibility</li> <li>• maintenance (software updates, downtime, staff expertise)</li> <li>• getting a service/storage up and running quickly</li> <li>• performance considerations</li> </ul>					
Learning Aim A: A2 – Impact of Modern Technologies					
Changes to modern teams facilitated by modern technologies: <ul style="list-style-type: none"> <li>• world teams (not bound by geographical restrictions, diversity)</li> <li>• multicultural</li> <li>• inclusivity (facilitation of member's needs)</li> <li>• 24/7/365 (no set work hours, team members in different time zones)</li> <li>• flexibility (remote working versus office based, permanent versus casual staff)</li> </ul>					
How modern technologies can be used to manage modern teams: <ul style="list-style-type: none"> <li>• collaboration tools</li> <li>• communication tools</li> <li>• scheduling and planning tools.</li> </ul>					
How organisations use modern technologies to communicate with stakeholders:					

<ul style="list-style-type: none"> <li>• communication platforms (website, social media, email, voice communication)</li> <li>• selection of appropriate communication channels (private/direct message, public status update) for sharing information, data and media.</li> </ul>					
<p>How modern technologies aid inclusivity and accessibility:</p> <ul style="list-style-type: none"> <li>• interface design (layout, font and colour selection)</li> <li>• accessibility features (screen reader support, alt text, adjustable typeface/font size, text to speech/'listen to this page')</li> <li>• flexibility of work hours and locations.</li> </ul>					
<p>Positive and negative impacts of modern technologies on organisations in terms of:</p> <ul style="list-style-type: none"> <li>• required infrastructure (communication technologies, devices, local and web-based platforms)</li> <li>• demand on infrastructure of chosen tools/platforms</li> <li>• availability of infrastructure</li> <li>• 24/7 access or security of distributed/dispersed data</li> <li>• collaboration or inclusivity (age, health, additional needs, multicultural)</li> <li>• accessibility (meeting legal obligations, provision requirements)</li> <li>• remote working</li> </ul>					
<p>Positive and negative impacts of modern technologies on individuals: flexibility (home/remote working)</p> <ul style="list-style-type: none"> <li>• working styles (choice of time, device, location)</li> <li>• impact on individual's mental wellbeing (depression, loneliness, self-confidence, separation from stressful environment, feel in control of own schedule, schedule adjusted to meet needs of family, less time commuting)</li> </ul>					
Learning Aim B: Cyber Security					
Learning Aim B: B1 – Threats to data					
<p>Why systems are attacked:</p> <ul style="list-style-type: none"> <li>• fun/challenge</li> <li>• industrial espionage or financial gain</li> <li>• personal attack</li> <li>• disruption</li> <li>• data/information theft</li> </ul>					
<p>External threats (threats outside the organisation) to digital systems and data security:</p> <ul style="list-style-type: none"> <li>• unauthorised access/hacking (black hat)</li> <li>• malware (virus, worms, botnet, rootkit, Trojan, ransomware, spyware)</li> <li>• denial of service attacks or phishing (emails, texts, phone calls)</li> <li>• pharming</li> <li>• social engineering</li> <li>• shoulder surfing</li> <li>• 'man-in-the-middle' attacks.</li> </ul>					
<p>Internal threats (threats within the organisation) to digital systems and data security:</p> <ul style="list-style-type: none"> <li>• unintentional disclosure of data</li> <li>• intentional stealing or leaking of information</li> <li>• users overriding security controls</li> <li>• use of portable storage devices</li> <li>• downloads from internet</li> <li>• visiting untrustworthy websites.</li> </ul>					

Impact of security breach: <ul style="list-style-type: none"> <li>• data loss</li> <li>• damage to public image</li> <li>• financial loss</li> <li>• reduction in productivity</li> <li>• downtime</li> <li>• legal action</li> </ul>					
Learning Aim B: B2 – Prevention and Management of threats to data					
User access restriction: <ul style="list-style-type: none"> <li>• physical security measures (locks)</li> <li>• passwords</li> <li>• using correct settings and levels of permitted access</li> <li>• biometrics</li> <li>• two-factor authentication (who you are, what you know, what you have).</li> </ul>					
Data level protection: <ul style="list-style-type: none"> <li>• firewall (hardware and software)</li> <li>• software/interface design (obscuring data entry, autocomplete, 'stay logged in')</li> <li>• anti-virus software</li> <li>• device hardening</li> <li>• procedures for backing up and recovering data</li> <li>• encryption of stored data (individual files, drive)</li> <li>• encryption of transmitted data.</li> </ul>					
Finding weaknesses and improving system security: <ul style="list-style-type: none"> <li>• ethical hacking (white hat, grey hat)</li> <li>• penetration testing</li> <li>• analyse system data/behaviours to identify potential risk</li> </ul>					
Learning Aim B: B3 – Policy					
Defining responsibilities: <ul style="list-style-type: none"> <li>• who is responsible for what</li> <li>• how to report concerns</li> <li>• reporting to staff/employees.</li> </ul>					
Defining security parameters: <ul style="list-style-type: none"> <li>• password policy</li> <li>• acceptable software/installation/usage policy</li> <li>• parameters for device hardening.</li> </ul>					
Disaster recovery policy: <ul style="list-style-type: none"> <li>• who is responsible for what</li> <li>• dos and don'ts for staff</li> <li>• defining the backup process (what is backed up, scheduling, media)</li> <li>• timeline for data recovery</li> <li>• location alternative provision (hardware, software, personnel)</li> </ul>					
Actions to take after an attack: <ul style="list-style-type: none"> <li>• investigate (establish severity and nature)</li> <li>• respond (inform/update stakeholders and appropriate authorities)</li> <li>• manage (containment, procedures appropriate to nature and severity)</li> <li>• recover (implement disaster recovery plan, remedial action)</li> <li>• analyse (update policy and procedures).</li> </ul>					
Learning Aim C: The Wider Implications of Digital Systems					
Learning Aim C: C1 – Responsible Use					

<p>Shared data (location-based data, transactional data, cookies, data exchange between services):</p> <ul style="list-style-type: none"> <li>• benefits of using shared data</li> <li>• drawbacks of using shared data</li> <li>• responsible use (legal considerations, privacy, ethical use).</li> </ul>					
<p>Environmental:</p> <ul style="list-style-type: none"> <li>• impact of manufacturing, use, and disposal of IT systems (energy, waste,</li> <li>• rare materials)</li> <li>• considerations when upgrading or replacing digital systems</li> <li>• usage and settings policies (auto power off, power-saving settings,</li> <li>• hard copy versus electronic distribution).</li> </ul>					
<p>Learning Aim C: C2 – Legal and ethical</p>					
<p>Importance of providing equal access to services and information:</p> <ul style="list-style-type: none"> <li>• benefits to organisations, individuals and society</li> <li>• legal requirements</li> <li>• professional guidelines/accepted standards.</li> </ul>					
<p>Net neutrality and how it impacts on organisations.</p>					
<p>The purpose and use of acceptable use policies:</p> <ul style="list-style-type: none"> <li>• scope – who the document applies to</li> <li>• assets – the equipment, documents, and knowledge covered by the policy</li> <li>• acceptable – behaviours that are expected/required by an organisation</li> <li>• unacceptable – behaviours that are not allowed by an organisation</li> <li>• monitoring – description of how behaviour is monitored by an organisation</li> <li>• sanctions – defining the processes and potential sanctions if unacceptable behaviour occurs</li> <li>• agreement – acknowledge (sign, click) that an individual agrees to abide by the policy.</li> </ul>					
<p>Blurring of social and business boundaries:</p> <ul style="list-style-type: none"> <li>• use of social media for business purposes</li> <li>• impact of personal use of digital systems (social media, web) on professional life</li> </ul>					
<p>Data protection principles:</p> <ul style="list-style-type: none"> <li>• lawful processing</li> <li>• collected only for specific purpose</li> <li>• only needed information is collected</li> <li>• should be accurate</li> <li>• kept only as long as is necessary</li> <li>• data subject rights</li> <li>• protected</li> <li>• data not transferred to countries with less protection</li> </ul>					
<p>Data and the use of the internet:</p> <ul style="list-style-type: none"> <li>• the right to be forgotten</li> <li>• appropriate and legal use of cookies and other transactional data</li> </ul>					
<p>Dealing with intellectual property:</p> <ul style="list-style-type: none"> <li>• the importance of intellectual property in organisations</li> <li>• methods of identifying/protecting intellectual property (trademarks, patents, copyright)</li> <li>• legal and ethical use of intellectual property (permissions, licensing, attribution)</li> </ul>					

<p>The criminal use of computer systems:</p> <ul style="list-style-type: none"> <li>• unauthorised access</li> <li>• unauthorised modification of materials</li> <li>• creation of malware</li> <li>• intentional spreading of malware</li> </ul>					
Learning Aim D: Planning and Communication in digital Systems					
Learning Aim D: D1 – Forms of notation					
<p>Understand how organisations use different forms of notation to explain systems, data and information:</p> <ul style="list-style-type: none"> <li>• data flow diagrams</li> <li>• flowcharts</li> <li>• system diagrams</li> <li>• tables</li> <li>• written information</li> </ul>					
<p>Be able to present knowledge and understanding using different forms of notations:</p> <ul style="list-style-type: none"> <li>• data flow diagrams</li> <li>• information flow diagrams</li> <li>• flowcharts</li> </ul>					