

**Student Learning Reflection & Personalised Learning Checklist**

|  |  |
| --- | --- |
| **Subject/Course:** | **BTEC ICT** |
| **Student Name:** |  |

|  |  |  |
| --- | --- | --- |
|  |  | Self Assessment |
| Topic | Key knowledge/skills | Red | Amber | Green |
| **Modern technologies** |
| 1. 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). |  |  |  |
| 2. a) 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). |  |  |  |
| 2. b) Features and uses of cloud computing: | Online applications |  |  |  |
| Consistency of version between users (features, file types) |  |  |  |
| Single shared instance of a file |  |  |  |
| Collaboration tools/features. |  |  |  |
| 3. a) 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) |  |  |  |
| 3. b) How cloud and ‘traditional’ systems are used together: | Available devices. |  |  |  |
| Device synchronisation |  |  |  |
| Online/offline working |  |  |  |
| Notifications. |  |  |  |
| 4. Implications for organisations when choosing cloud technologies: | Consideration of disaster recovery policies (service provider’s, organisation’s) |  |  |  |
| 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 |  |  |  |
| Performance considerations (responsiveness to user, complexity of task, available |  |  |  |
| Devices and communication technologies). |  |  |  |
| **Impact of Modern Technologies** |
| 1. 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). |  |  |  |
| 2. How modern technologies can be used to manage modern teams: | Collaboration tools |  |  |  |
| Communication tools |  |  |  |
| Scheduling and planning tools. |  |  |  |
| 3a. 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. |  |  |  |
| 3b. 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. |  |  |  |
| 4a. 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 |  |  |  |
| 4a. Positive and negative impacts of modern technologies on organisations in terms of: | 24/7 access |  |  |  |
| Security of distributed/disbursed data |  |  |  |
| Collaboration |  |  |  |
| Inclusivity (age, health, additional needs, multicultural) |  |  |  |
| Accessibility (meeting legal obligations, provision requirements) |  |  |  |
| Remote working. |  |  |  |
| 5. 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-confidence, separation from stressful environment, feel in control of own schedule, schedule adjusted to meet needs of family, less time commuting). |  |  |  |
| **Cyber security**  |
| **Threats to data** |
| 1. Why systems are attacked: | Fun/challenge |  |  |  |
| Industrial espionage |  |  |  |
| Financial gain |  |  |  |
| Personal attack |  |  |  |
| Disruption |  |  |  |
| Data/information theft. |  |  |  |
| 2. 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. |  |  |  |
| 3a) 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 |  |  |  |
| 3b) Impact of security breach: | Data loss |  |  |  |
| Damage to public image |  |  |  |
| Financial loss |  |  |  |
| Reduction in productivity |  |  |  |
| Downtime |  |  |  |
| Legal action |  |  |  |

|  |  |  |
| --- | --- | --- |
|  |  | Self Assessment |
| Topic | Key knowledge/skills | Red | Amber | Green |
| **Cyber security** |
| **Prevention and management of threats to data**  |
| 1. 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). |  |  |  |
| 2. Data level protection: | Firewall (hardware and software) |  |  |  |
| Software/interface design (obscuring data entry, autocomplete, ‘stay logged in’) |  |  |  |
| Anti-virus software |  |  |  |
| Device hardening |  |  |  |
| Procedures for backing up and recovering data |  |  |  |
| Encryption of stored data (individual files, drive) |  |  |  |
| Encryption of transmitted data. |  |  |  |
| 3. Finding weaknesses and improving system security: | Ethical hacking (white hat, grey hat) |  |  |  |
| Penetration testing |  |  |  |
| Analyse system data/behaviours to identify potential risks. |  |  |  |
| **Policy**  |
| 1. Defining responsibilities and security parameters: | Who is responsible for what |  |  |  |
| How to report concerns |  |  |  |
| Reporting to staff/employees. |  |  |  |
| Password policy |  |  |  |
| Acceptable software/installation/usage policy |  |  |  |
| Parameters for device hardening. |  |  |  |
| 2. Disaster recovery policy and actions to take after an attack: | 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). |  |  |  |
| 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). |  |  |  |

|  |
| --- |
| **The wider implications of digital systems** |
| **Responsible use:** | Red | Amber | Green |
| 1. 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, privacy, ethical use). |  |  |  |
| 2. 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). |  |  |  |
| **Legal and ethical**  |
| 1a) Importance of providing equal access to services and information: | Benefits to organisations, individuals and society |  |  |  |
| Legal requirements |  |  |  |
| Professional guidelines/accepted standards. |  |  |  |
| 1b) Net neutrality and how it impacts on organisations. |  |  |  |
| 2a) 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 |  |  |  |
| 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 |  |  |  |
| 2b) 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. |  |  |  |
| 3. 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. |  |  |  |
| The right to be forgotten |  |  |  |
| Appropriate and legal use of cookies and other transactional data. |  |  |  |
| 4. Dealing with intellectual property and the criminal use of computer systems: | 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). |  |  |  |
| Unauthorised access |  |  |  |
| Unauthorised modification of materials |  |  |  |
| Creation of malware |  |  |  |
| Intentional spreading of malware. |  |  |  |
| **Planning and communication in digital systems** |
| **Forms of notation**  |
| 1. Use of different forms of notation: | Data flow diagrams |  |  |  |
| Flowcharts |  |  |  |
| System diagrams |  |  |  |
| Tables |  |  |  |
| Written information |  |  |  |
| 2. Data flow Diagrams |  |  |  |
| 3. Information flow diagrams |  |  |  |
| 4. Flowcharts. |  |  |  |