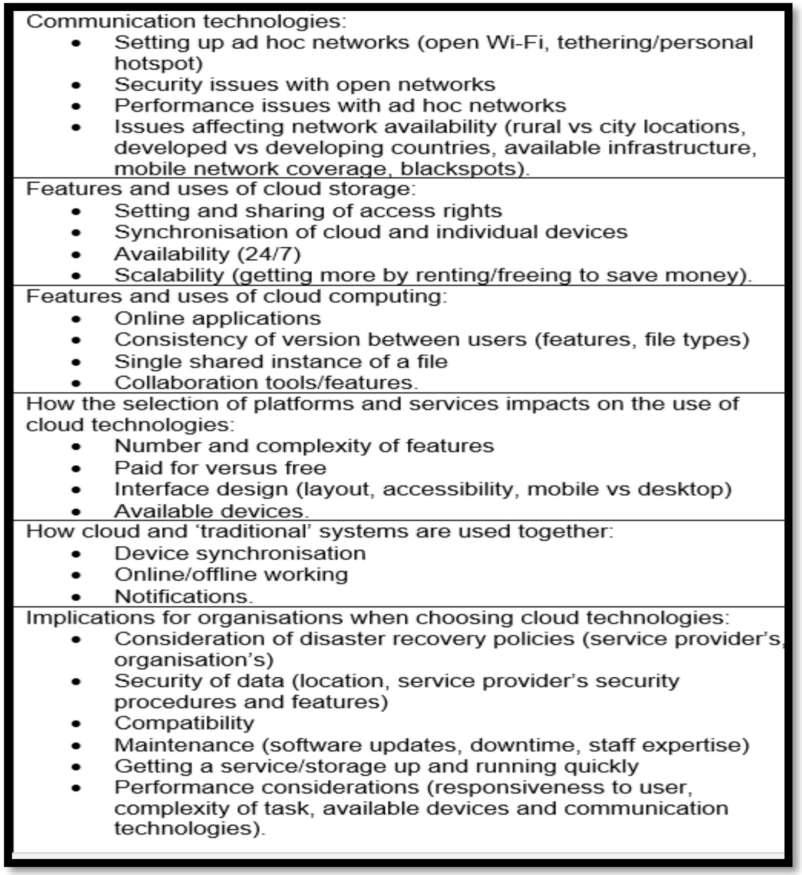
Subject: IT

Topic: Component 3 - Learning Aim A: Modern Technologies

Summary of key information:

Modern Technologies



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).

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).

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.

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)
- Available devices.

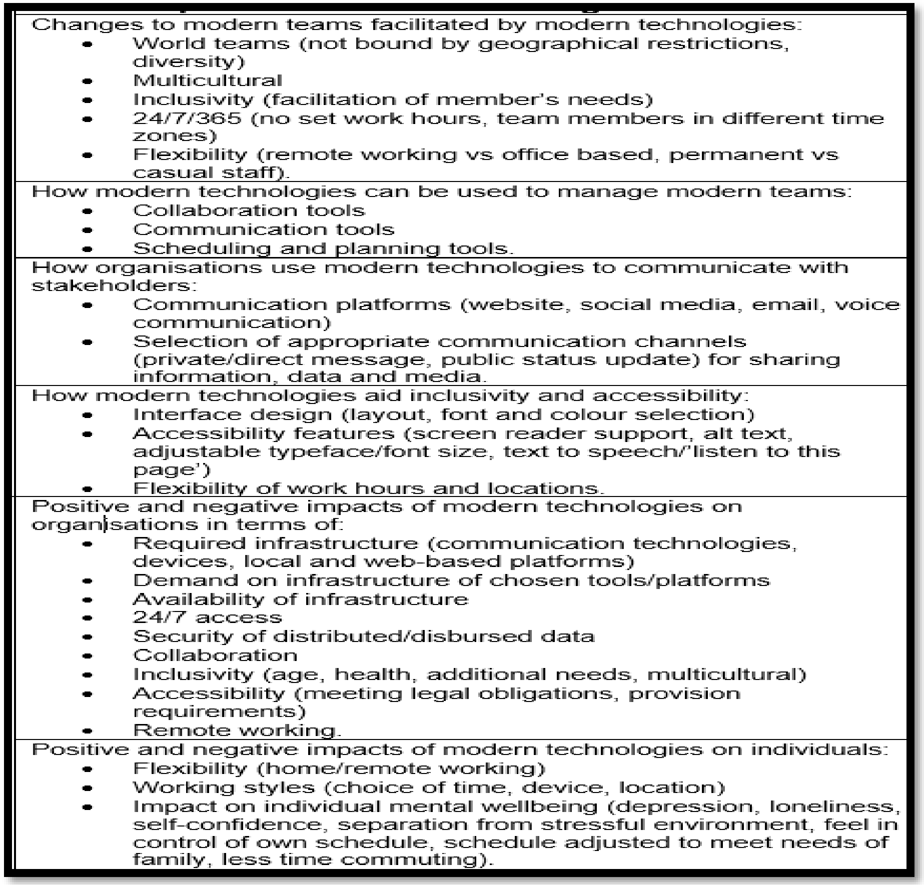
How cloud and 'traditional' systems are used together:

- Device synchronisation
- Online/offline working
- Notifications.

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



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).

How modern technologies can be used to manage modern teams:

- Collaboration tools
- Communication tools
- Scheduling and planning tools.

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.

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.

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
- 24/7 access
- Security of distributed/disbursed data
- Collaboration
- Inclusivity (age, health, additional needs, multicultural)
- Accessibility (meeting legal obligations, provision requirements)
- Remote working.

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).

Key terms: Bluetooth, Ad Hoc Network, Personal Area Network, Tethering, Personal Hotspot, PIN, Encrypted, USB, Insecure Connections, Streaming, Server, Downloading, Uploading, Synchronising, Scalability, Stakeholders, Downtime, Geo-data, Virtual Machines, System Administrator, Spam, Version Control, URL, ALT Text, Distributed Data, Dispersed Data, Wiki.

Subject: IT

Topic: Component 3 - Learning Aim B: Cyber Security

Summary of key information:

Threats to Data

Why systems are attacked:

- Fun/challenge
- Industrial espionage
- Financial gain
- Personal attack
- Disruption
- Data/information theft

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

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

Impact of security breach:

- Data loss
- Damage to public image
- Financial loss
- Reduction in productivity
- Downtime
- Legal action

Prevention and Management of Threats to Data

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)

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

Finding weaknesses and improving system security:

- Ethical hacking (white hat, grey hat)
- Penetration testing
- Analyse system data/behaviours to identify potential risks

Policy

Defining responsibilities:

- Who is responsible 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 (what is backed up, scheduling, media)
- Timeline for data recovery
- Location alternative provision (hardware, software, personnel)

Actions to take after an attack:

- 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)

Key terms: Intellectual Property, Ransomware, Malware, Denial-of-Service Attacks, Social Engineering, Phishing, Pharming, Productivity, Swipe Card, Firewall, Local Area Network, Access Control List, Shoulder Surfing, Session Cookies, Worms, Trojans, Rootkit, Spyware, Vulnerable System, Security Patches, Privilege, Default Password, Software Audit, Data Protection Controller.