Non-Negotiables: *Learning Aim A*

1	Q: Give the examples of communication technologies. A: Setting up ad hoc networks (open Wi-Fi, tethering/personal hotspot), security issues with open networks, performance issues with ad hoc networks, and issues affecting network availability.
2	Q: Give the features and uses of cloud storage. A: Setting and sharing access rights, synchronisation of cloud and individual devices, 24/7 availability and scalability.
3	Q: Give the features and uses of cloud computing. A: Online applications, consistency of version between users, a single shared instance of a file, and collaboration tools/features.
4	Q: Give the factors that influence the selection of cloud platforms and services. A: Number and complexity of features, paid-for versus free services, interface design and available devices.
5	Q: Describe how cloud and traditional systems are used together. A: Device synchronisation, online and offline working, and notifications.
6	Q: Give the implications for organisations when choosing cloud technologies. A: Disaster recovery policies, security of data, compatibility maintenance, rapid deployment of services and performance considerations.
7	Q: Give the changes to modern teams facilitated by modern technologies. A: World teams, multicultural teams, inclusivity, 24/7/365 working and flexibility.
8	Q: Give the ways modern technologies can be used to manage teams. A: Collaboration tools, communication tools and scheduling and planning tools.
9	Q: Describe how organisations use modern technologies to communicate with stakeholders. A: Using websites, social media, email and voice communication, and selecting appropriate communication channels for sharing information, data and media.
10	Q: Give the positive and negative impacts of modern technologies on individuals. A: Flexibility through remote working, different working styles, impacts on mental wellbeing, reduced commuting, improved control over schedules, but also potential loneliness, depression and reduced self-confidence.

Non-Negotiables: *Learning Aim B*

1	Q: Give the reasons why systems are attacked. A: Fun or challenge, industrial espionage or financial gain, personal attack, disruption, and data or information theft.
2	Q: Give the external threats to digital systems and data security. A: Unauthorised access or hacking, malware, denial of service attacks, phishing, pharming, social engineering, shoulder surfing and man-in-the-middle attacks.
3	Q: Give the types of malware. A: Virus, worms, botnet, rootkit, Trojan, ransomware and spyware.
4	Q: Give the internal threats to digital systems and data security. A: Unintentional disclosure of data, intentional stealing or leaking of information, users overriding security controls, use of portable storage devices, downloads from the internet and visiting untrustworthy websites.
5	Q: Give the impacts of a security breach. A: Data loss, damage to public image, financial loss, reduction in productivity, downtime and legal action.
6	Q: Give the methods used to restrict user access. A: Physical security measures, passwords, correct settings and access levels, biometrics and two-factor authentication.
7	Q: Give the methods used for data-level protection. A: Firewalls, software and interface design features, anti-virus software, device hardening, backup and recovery procedures, encryption of stored data and encryption of transmitted data.
8	Q: Give the ways weaknesses can be identified and system security improved. A: Ethical hacking, penetration testing and analysing system data and behaviours to identify risks.
9	Q: Give the areas covered by a security policy. A: Defining responsibilities, defining security parameters and disaster recovery policies.
10	Q: Give the actions to take after a cyber attack. A: Investigate, respond, manage, recover and analyse.

Non-Negotiables: *Learning Aim C*

1	Q: Give the types of shared data used by digital systems. A: Location-based data, transactional data, cookies and data exchange between services.
2	Q: Describe the considerations relating to the environmental impact of digital systems. A: The impact of manufacturing, use and disposal of IT systems, considerations when upgrading or replacing systems, and usage and settings policies such as power-saving features and electronic distribution.
3	Q: Explain why equal access to services and information is important. A: It benefits organisations, individuals and society, helps meet legal requirements and follows professional guidelines and accepted standards.
4	Q: Explain what net neutrality is. A: Net neutrality is the principle that internet service providers should treat all internet traffic equally without discrimination.
5	Q: Give the sections of an acceptable use policy. A: Scope, assets, acceptable behaviour, unacceptable behaviour, monitoring, sanctions and agreement.
6	Q: Describe how social and business boundaries can become blurred. A: Through the use of social media for business purposes and the impact of personal use of digital systems on professional life.
7	Q: Give the data protection principles. A: Lawful processing, collected only for a specific purpose, only necessary information collected, accuracy, retained only as long as necessary, data subject rights, protection of data and restrictions on transfers to countries with less protection.
8	Q: Give the ways data and the internet are regulated. A: The right to be forgotten and the appropriate and legal use of cookies and other transactional data.
9	Q: Give the methods used to identify and protect intellectual property. A: Trademarks, patents and copyright.
10	Q: Give the examples of criminal use of computer systems. A: Unauthorised access, unauthorised modification of materials, creation of malware and intentional spreading of malware.