

11

CHAPTER

ETHICAL, SOCIAL AND LEGAL CONCERNS IN COMPUTER USAGE



Topic No.	Title	Page No.
11.1	Responsible Computer Usage	287
11.2	Safe and Secure Operations of Digital Platforms	287
11.3	Best Practices in Online Behaviour	290
11.4	Legal and Ethical Frameworks	292
11.5	Intellectual Property Rights	295
11.6	Responsible Internet Use	300
11.7	Impact of Computing on Society	300
*	Summery	303
*	Exercise	304
*	Answer Keys	308

11.1 RESPONSIBLE COMPUTER USAGE**11.2 SAFE AND SECURE OPERATION OF DIGITAL PLATFORMS****LONG QUESTION**

Q. 21 What are the key aspects of responsible computer usage and why is it important to choose the right hardware and software?

Ans: Responsible computer usage involves making thoughtful decisions when using technology, focusing on selecting the appropriate hardware and software, safeguarding data, and respecting others while using the internet.

1. Choosing the Right Hardware and Software: Hardware refers to the physical components of a computer, such as the monitor, keyboard, and CPU, while software includes the programs and applications, like word processors and games. Selecting the right hardware and software is crucial because it impacts the safety, efficiency, and overall user experience of a computer.

2. Safety: Using outdated or insecure hardware or software can put users at risk, as it may expose the system to threats like viruses or hackers. For instance, an outdated antivirus program could fail to protect personal information from cyberattacks.

3. Efficiency: The right hardware and software enhance task performance. For example, a modern computer with updated software can run newer programs smoothly, whereas using an old computer to play new video games could result in slow performance or failure to function properly.

4. Compatibility: Compatibility between hardware and software is vital. Ensuring that the system requirements of the software match the specifications of the computer is important to avoid issues such as crashes or inefficient operation.

Q. 22 What steps can be taken to ensure the safe and secure operation of digital platforms devices?

Ans: The safe and secure operation of digital platforms and devices involves several critical practices aimed at protecting personal information, preventing security threats, and maintaining a positive online experience.

1. Safe Operation of Digital Platforms and Devices:

Using Strong Passwords: Create strong, unique passwords combining letters, numbers, and special characters. For example, instead of "password123," opt for "B3tt3rP@ssw0rd!" to improve security.

Regular Software Updates: Keeping devices and applications up to date is crucial for security. Updates often include important security patches that help protect against new threats.

Being Cautious with Links and Downloads: Avoid clicking on unknown links or downloading files from untrusted sources, as these could contain malware that compromises your device and data.

Understanding Privacy Settings: Adjust privacy settings to control who can access your information and interact with you online, safeguarding your personal details.

Avoiding Oversharing: Be mindful of the information you share online. Refrain from posting personal details such as your home address or phone number.

2. Secure Use of Digital Platforms:

Two-Factor Authentication (2FA): Add an extra layer of security to your accounts by using 2FA. This requires providing additional information, like a code sent to your phone, making it harder for hackers to gain access.

Avoiding Public Wi-Fi for Sensitive Transactions: Public Wi-Fi networks are often less secure, so it's best to avoid conducting sensitive activities, like online banking, while using them.

Being Aware of Scams: Online scams, including phishing emails, can trick you into revealing personal information. Always verify the source before responding to unsolicited requests.

Regularly Reviewing Account Activity: Periodically check your accounts for suspicious activity, and if anything unusual is found, change your password immediately and report it.

Backing Up Important Data: Regular backups of data prevent loss due to device failure. Use external drives or cloud storage services like Google Drive or Dropbox for secure backups.

SHORT QUESTIONS

Q. 38 What does responsible computer usage mean?

Ans: RESPONSIBLE COMPUTER USAGE

Responsible computer usage involves selecting appropriate hardware and software, protecting personal information, and behaving respectfully online.

Q. 39 Why is choosing compatible hardware and software important?

Ans: COMPATIBLE HARDWARE AND SOFTWARE

Compatibility ensures smooth operation, better efficiency, and an enhanced user experience.

Example: Installing a high-end game on an incompatible computer may cause it to crash.

Q. 40 What are strong passwords, and why are they important?

Ans: STRONG PASSWORDS

Strong passwords include a mix of letters, numbers, and symbols. They protect accounts from unauthorized access.

Example: "S3cureP@ssw0rd!"

Q. 41 How can regular software updates enhance security?

Ans: REGULAR SOFTWARE UPDATES

Updates fix bugs and address security vulnerabilities, protecting devices from new threats.

Example: Windows updates include patches for virus protection.

Q. 42 What is online etiquette?

Ans: ONLINE ETIQUETTE

It is treating others with respect and maintaining positive interactions online.

Example: Avoiding rude comments in discussions.

Q. 43 Why should oversharing personal details online be avoided?

Ans: PERSONAL DETAILS

Oversharing increases risks of identity theft or misuse.

Example: Sharing your home address publicly could lead to security issues.

Q. 44 What is Two-Factor Authentication (2FA), and how does it help?

Ans: TWO-FACTOR AUTHENTICATION (2FA)

2FA adds a second layer of account security by requiring an additional verification step.

Example: Entering a code sent to your phone after the password.

Q. 45 How does backing up data ensure safety?

Ans: BACKING UP DATA

It prevents data loss in case of device failure or cyber-attacks.

Example: Saving files to Google Drive.

Q. 46 What are phishing scams, and how can you avoid them?

Ans: PHISHING SCAMS, AND HOW CAN YOU AVOID THEM

Phishing scams trick users into sharing personal information through fake emails or links. Avoid clicking suspicious links and verify sources.

Q. 47 Why is it risky to use public Wi-Fi for sensitive transactions?

Ans: PUBLIC WI-FI FOR SENSITIVE TRANSACTIONS

Public Wi-Fi lacks security, making it easier for hackers to intercept your data.

Example: Avoid accessing online banking on public networks.

Q. 48 What is malware, and how can it affect devices?

Ans: MALWARE

Malware is malicious software that can steal information or damage devices.

Example: A virus sent through email attachments.

Q. 49 What does “cyber hygiene” refer to, and why is it important?

Ans: It refers to maintaining good digital practices, like updating antivirus software, to prevent cyber threats.

Q. 50 What should you review in your account activity regularly?

Ans: ACCOUNT ACTIVITY

Look for unusual logins, messages, or transactions to detect unauthorized access.

Q. 51 How do privacy settings protect you online?

Ans: PRIVACY SETTINGS

They control who can see your information and interact with you, reducing risks of misuse.

Q. 52 Why is respectful behavior online crucial?

Ans: RESPECTFUL BEHAVIOR

It fosters positive interactions and prevents misunderstandings or conflicts.

MULTIPLE CHOICE QUESTIONS

- **What does safe computer usage include?**
 - (A) Using any hardware and software
 - (B) Sharing passwords
 - (C) Protecting personal information
 - (D) Ignoring software updates
- **What does hardware refer to in a computer?**
 - (A) Programs and applications
 - (B) Physical components like monitor and keyboard
 - (C) Cloud storage services
 - (D) Internet browsers
- **What does a strong password typically include?**
 - (A) Only letters
 - (B) Letters, numbers, and special characters
 - (C) Just your name and birthdate
 - (D) Simple, easy-to-guess words
- **Why is regular software updating important?**
 - (A) It improves hardware design
 - (B) It fixes security vulnerabilities
 - (C) It deletes unused applications
 - (D) It stops viruses permanently
- **What does compatibility in hardware and software mean?**
 - (A) They must have the same brand
 - (B) They should work well together
 - (C) They should have similar designs
 - (D) They must be used simultaneously
- **What should you avoid doing on public Wi-Fi?**
 - (A) Browsing websites
 - (B) Checking emails
 - (C) Conducting sensitive transactions
 - (D) Watching videos
- **What is Two-Factor Authentication (2FA)?**
 - (A) A stronger antivirus software
 - (B) A second layer of security for accounts
 - (C) A backup software
 - (D) A type of password storage
- **Which of these is an example of online etiquette?**
 - (A) Sharing all personal details
 - (B) Treating others with respect
 - (C) Ignoring others' opinions
 - (D) Posting mean comments
- **What should you check before clicking a link?**
 - (A) Its color
 - (B) Its length
 - (C) Its source
 - (D) Its language
- **Why is it important to review account activity regularly?**
 - (A) To delete old accounts
 - (B) To check for unusual activity
 - (C) To increase your followers
 - (D) To update your profile picture
- **What should you avoid oversharing online?**
 - (A) Hobbies
 - (B) Personal details like home address
 - (C) Favorite movies
 - (D) School subjects
- **What can malware do?**

- (A) Protect your data
- (B) Steal your personal information
- (C) Enhance your device's speed
- (D) Delete unused apps
- **What is a benefit of backing up data?**
 - (A) Faster computer performance
 - (B) Prevents data loss
 - (C) Stops malware
 - (D) Enhances display resolution
- **Which of these helps in safer internet use?**
 - (A) Ignoring scam emails
 - (B) Updating software regularly
 - (C) Sharing passwords with friends
 - (D) Using outdated devices
- **What does "cyber hygiene" refer to?**
 - (A) Cleaning your keyboard
 - (B) Regularly updating antivirus software
 - (C) Posting frequently on social media
 - (D) Using public Wi-Fi for banking

11.3 BEST PRACTICES IN ONLINE BEHAVIOUR

LONG QUESTION

26. Discuss the importance of best practices in online behavior, focusing on responsible use, privacy settings, and data security. Provide examples.

Ans: **Responsible Use of Digital Platforms**

Social Media: Avoid sharing personal information like addresses or phone numbers.

Example: Share vacation photos only with friends instead of making them public.

Email: Be cautious of emails from unknown senders to avoid phishing scams or malware.

Example: Delete emails with suspicious links or attachments.

Cloud Services: Use strong passwords and avoid storing sensitive information.

Example: Use Dropbox with Two-Factor Authentication for added security.

Online Applications: Download apps only from trusted sources to avoid harmful software.

Example: Install educational apps from verified stores like Google Play Store.

Importance of Privacy Settings

Control Access: Privacy settings let you decide who can view your personal information.

Example: On Facebook, choose "Friends Only" for posts.

Regular Updates: Update settings periodically to keep up with changes in platform policies.

Example: Adjust privacy settings when new features are introduced.

Data Security Measures

Strong Passwords: Protect your accounts with passwords that combine letters, numbers, and symbols.

Example: Use "T3ch!S@fe" instead of simple passwords.

Informed Consent: Understand how your data is collected and used by digital platforms.

Example: Review terms and conditions before signing up for a service.

By following these best practices, users can enjoy the benefits of digital platforms while ensuring safety and ethical behavior online.

SHORT QUESTIONS

- Q. 4 What is responsible online behavior?

Ans: **RESPONSIBLE ONLINE BEHAVIOR**

Responsible online behavior involves thinking before posting, avoiding sharing personal information, and respecting others' privacy.

Example: Avoid posting your home address publicly.

- Q. 5 Why is it important to avoid emails from unknown senders?

Ans: **IMPORTANT TO AVOID EMAILS FROM UNKNOWN SENDERS**

Emails from unknown senders can contain harmful links or attachments that might install malware or steal your information.

Q. 6 What are cloud services, and how should they be used responsibly?

Ans: SERVICES, AND HOW SHOULD THEY BE USED RESPONSIBLY

Cloud services store and share files online. Use strong passwords and avoid sharing sensitive data to ensure security.

Example: Use Google Drive with a secure password to protect your documents.

Q. 7 What are the risks of downloading applications from unverified sources?

Ans: DOWNLOADING APPLICATIONS FROM UNVERIFIED SOURCES

Applications from unverified sources may contain malware or harmful software.

Example: Download apps only from the Google Play Store or Apple App Store.

Q. 8 What is the purpose of privacy settings?

Ans: PURPOSE OF PRIVACY SETTINGS

Privacy settings control who can see your information and help protect personal data from unauthorized access.

Why is it important to regularly review privacy settings?

Ans: IMPORTANT TO REGULARLY REVIEW PRIVACY SETTINGS

Regularly reviewing settings ensures your personal information remains protected as platforms update their policies.

Q. 9 How does "informed consent" relate to data collection?

Ans: "INFORMED CONSENT" RELATE TO DATA COLLECTION

Informed consent ensures users know how their data is being used and shared, promoting ethical data practices.

Q. 10 What are the benefits of using strong, unique passwords?

Ans: BENEFITS OF USING STRONG, UNIQUE PASSWORDS

Strong passwords make it harder for unauthorized users to access your accounts.

Example: Use "S3cur3!Passw0rd" instead of "password123."

Q. 11 Why should personal information not be shared on social media?

Ans: PERSONAL INFORMATION NOT BE SHARED ON SOCIAL MEDIA

Sharing personal information publicly can lead to identity theft or misuse.

Q. 12 What should you do before posting anything on social media?

Ans: POSTING ANYTHING ON SOCIAL MEDIA

Think carefully about the content, ensuring it does not reveal personal details or harm others.

MULTIPLE CHOICE QUESTIONS

Q.12 What should you avoid sharing on social media?

(A) Your favorite movie

(B) Your home address

(C) Pictures of nature

(D) Your daily routine

Q.13 What is a safe way to handle emails?

(A) Open all attachments

(B) Avoid emails from unknown senders

(C) Reply to every email immediately

(D) Share passwords via email

Q.14 Why is it important to use strong passwords for cloud services?

(A) To make them easy to remember

(B) To protect sensitive data

(C) To allow faster file uploads

(D) To avoid frequent logins

Q.15 Where should you download online applications?

(A) Any website offering free downloads

(B) Google Play Store or Apple App Store

(C) From random pop-up ads

(D) Peer-to-peer sharing platforms

Q.16 What should you do before posting on social media?

(A) Share as much personal information as possible

(B) Think carefully about what you are posting

(C) Ignore privacy settings

(D) Post without consideration

Q.17 What can harmful email attachments contain?

(A) Useful links

(B) Malware

(C) Fun quizzes

(D) Free apps

- Q.18 What do privacy settings allow you to control?**
 (A) The speed of your internet connection (B) Who can see your personal information
 (C) The appearance of your profile (D) Your app's download speed
- Q.19 What should you regularly review on social media?**
 (A) Profile pictures (B) Privacy settings
 (C) Post comments (D) Friend requests
- Q.20 What is "informed consent" in data collection?**
 (A) Knowing how your data will be used (B) Ignoring data usage policies
 (C) Allowing all data sharing (D) Using weak passwords
- Q.21 Why is it risky to share sensitive data through cloud storage?**
 (A) It takes up storage space (B) It can be accessed by unauthorized users
 (C) It reduces upload speed (D) It creates duplicate files
- Q.22 What is the primary use of cloud services?**
 (A) Playing games (B) Storing and sharing files
 (C) Watching videos (D) Sending emails
- Q.23 What should you avoid doing with online applications?**
 (A) Downloading from trusted sources (B) Using strong passwords
 (C) Downloading from unverified websites (D) Reading reviews before downloading
- Q.24 What is the benefit of regularly updating privacy settings?**
 (A) Faster internet speed (B) Protecting personal information
 (C) Increasing your followers (D) Accessing free features
- Q.25 How can you secure your online accounts?**
 (A) Use the same password for all accounts (B) Use strong, unique passwords
 (C) Share passwords with friends (D) Avoid changing passwords frequently
- Q.26 What does responsible online behavior include?**
 (A) Ignoring data security (B) Sharing all posts publicly
 (C) Thinking before posting (D) Using weak passwords

11.4 LEGAL AND ETHICAL FRAMEWORKS

LONG QUESTION

- 45. Discuss the importance of legal and ethical frameworks in data handling, focusing on privacy laws, data ethics principles, and ethical guidelines for data usage. Provide examples.**

Ans:

1. Privacy Laws

Definition:

Rules set by the government to protect personal information.

Purpose:

Ensure responsible data handling and provide legal actions for misuse.

Example:

If a company shares your data without permission, privacy laws enable you to seek justice.

2. Principles of Data Ethics

Transparency:

Be clear about how data is used.

Example:

A website informs users before tracking their activity.

Respect for Privacy:

Protect personal information from unauthorized access.

Example:

Encrypting sensitive data like medical records.

Accountability:

Take responsibility for any misuse or breaches.

Example:

Informing users of a data breach and fixing it promptly.

3. Ethical Guidelines for Data Usage**Informed Consent:**

Always ask for user permission before collecting data.

Example:

A survey asks participants to agree before sharing information.

Data Minimization:

Only collect necessary data to reduce misuse risks.

Example:

A shopping website asks for email but not personal health details.

Data Security:

Use encryption and strong passwords to protect collected data.

Example:

Banks encrypt customer financial data.

Accountability:

Address issues responsibly in case of a breach.

Example:

A company affected by a breach compensates users and updates security.

By following these frameworks, we ensure ethical and secure data handling while building trust in digital platforms.

SHORT QUESTIONS**Q.1 What are privacy laws?**

Ans:

PRIVACY LAWS

Privacy laws are government rules designed to protect personal information and ensure responsible data handling.

Q.2 What are the consequences of unauthorized access to data?

Ans:

CONSEQUENCES OF UNAUTHORIZED ACCESS TO DATA

Unauthorized access can lead to identity theft, fraud, and legal penalties for the offender.

What is data ethics?

Ans:

DATA ETHICS

Data ethics involves the fair and responsible collection, storage, and use of information while respecting individuals' rights.

Q.3 What is "informed consent" in data collection?

Ans:

INFORMED CONSENT" IN DATA COLLECTION

Informed consent means seeking user permission before collecting their data and informing them about its use.

Q.4 Why is data security important in data storage?

Ans:

DATA SECURITY IN DATA STORAGE

Data security prevents unauthorized access, ensuring personal and sensitive data remains protected.

Q.5 What is transparency in data ethics?

Ans:

TRANSPARENCY IN DATA ETHICS

Transparency involves being clear about how data is collected, used, and stored.

Q.6 What are the ethical considerations in data sharing?

Ans:

ETHICAL CONSIDERATIONS IN DATA SHARING

Data sharing must respect user consent, minimize unnecessary information exchange, and avoid harm to others.

Q.7 What is accountability in data ethics?

Ans:

ACCOUNTABILITY IN DATA ETHICS

Accountability involves taking responsibility for data misuse or breaches and fixing the issues.

Q.8 What is the significance of data minimization?

Ans: SIGNIFICANCE OF DATA MINIMIZATION

Data minimization limits data collection to only what is necessary, reducing risks of misuse or breaches.

Q.9 What is a data breach?

Ans: DATA BREACH

A data breach occurs when sensitive or personal information is exposed without authorization.

MULTIPLE CHOICE QUESTIONS

Q.34 What is the primary purpose of privacy laws?

- (A) To share personal data
- (B) To protect personal information
- (C) To promote public communication
- (D) To increase data usage

Q.35 What does "unauthorized access" to personal information mean?

- (A) Access with user permission
- (B) Legal use of data
- (C) Access without user permission
- (D) Sharing information with consent

Q.36 What can unauthorized access lead to?

- (A) Stronger security measures
- (B) Identity theft or fraud
- (C) Faster data sharing
- (D) Enhanced privacy laws

Q.37 What principle is NOT part of data ethics?

- (A) Transparency
- (B) Accountability
- (C) Ignoring privacy
- (D) Respect for privacy

Q.38 What does "informed consent" in data ethics mean?

- (A) Asking for permission before collecting data
- (B) Collecting data without informing the user
- (C) Sharing data without restriction
- (D) Hiding the purpose of data collection

Q.39 Which of the following is an example of ethical data storage?

- (A) Using encryption to secure sensitive data
- (B) Leaving personal records unsecured
- (C) Sharing medical data with unauthorized people
- (D) Deleting all stored data regularly

Q.40 What should a school avoid sharing without permission?

- (A) Student grades
- (B) Class schedules
- (C) School policies
- (D) Holiday announcements

Q.41 What is an unethical use of collected data?

- (A) Using data only for its intended purpose
- (B) Selling data to third parties without consent
- (C) Protecting data with encryption
- (D) Minimizing unnecessary data collection

Q.42 What should be prioritized in data security?

- (A) Sharing passwords
- (B) Avoiding encryption
- (C) Using strong passwords and encryption
- (D) Ignoring potential breaches

Q.43 What is data minimization?

- (A) Collecting as much data as possible
- (B) Limiting data collection to what is necessary
- (C) Sharing data with everyone
- (D) Deleting all collected data

Q.44 What happens when companies fail to protect user data?

- (A) They gain more customers
- (B) They face legal penalties
- (C) They are exempt from responsibility
- (D) They automatically update security measures

Q.45 What is an example of transparency in data ethics?

- (A) Keeping data usage hidden
- (B) Being clear about how data is used
- (C) Avoiding responsibility for data breaches
- (D) Encrypting all public information

Q.46 What does accountability in data ethics require?

- (A) Ignoring breaches
- (B) Taking responsibility for mistakes
- (C) Hiding security issues
- (D) Avoiding communication with users

Q.47 What does the term "data breach" refer to?

- (A) Securing information
- (B) Unauthorized exposure of data
- (C) Updating security policies
- (D) Legal data sharing

Q.48 What is an example of ethical data sharing?

- (A) Sharing data without user knowledge (B) Sharing sensitive data only when necessary
(C) Selling personal data to advertisers (D) Posting user data online publicly

11.5 INTELLECTUAL PROPERTY RIGHTS

LONG QUESTIONS

Q. 4 Explain the concepts of copyright, trademarks, and patents, along with their significance in protecting digital content.

1. Copyright

Definition:

A legal right protecting original works like books, music, and software.

Significance:

Ensures creators have control over the use of their creations.

Example:

Authors can decide how their books are distributed or adapted.

2. Trademarks

Definition:

Unique symbols or slogans distinguishing a company's products or services.

Significance:

Protects brand identity and prevents customer confusion.

Example:

Nike's "swoosh" logo.

3. Patents

Definition: Exclusive rights protecting new inventions or processes.

Significance: Prevents unauthorized use or sale of inventions.

Example: Patenting a new smartphone technology.

Q. 5 What strategies can be used to prevent internet addiction and foster healthy online habits?

Ans: Introduction

Internet addiction is a growing concern in today's digital world. It occurs when excessive time spent online interferes with daily responsibilities, relationships, and mental health. Preventing internet addiction and fostering healthy online habits involves understanding the risks and adopting balanced strategies for digital well-being.

Recognizing Signs of Internet Addiction

The first step to prevention is identifying symptoms of internet addiction. These include:

Difficulty in limiting online time.

Neglecting daily tasks, like studying or spending time with family.

Feeling anxious or restless when not connected to the internet.

Example: A teenager who spends hours gaming and skips meals or homework might be showing signs of internet addiction.

Setting Time Limits

Establishing time boundaries for internet usage is crucial to maintaining a balance.

Use time-tracking apps to monitor screen time.

Create a daily or weekly schedule for online activities.

Example: Allocating one hour per day for social media and taking breaks during long work sessions can reduce excessive internet use.

Engaging in Offline Activities

Balancing online and offline life is essential for mental and physical well-being.

Participate in activities like sports, reading, or spending time with family.

Cultivate hobbies that do not involve digital devices.

Example: Joining a sports team or learning to play a musical instrument provides constructive alternatives to being online.

Taking Regular Breaks

Extended online sessions can lead to fatigue and addiction. Regular breaks help maintain focus and reduce dependency.

Follow the "20-20-20 rule": Every 20 minutes, look at something 20 feet away for 20 seconds.

Take short breaks after completing tasks online.

Example: A student studying online can take a 5-minute break every hour to stretch and relax their eyes.

Using Technology Wisely

Technology can help manage screen time and prevent addiction.

Install apps that limit time spent on social media or games.

Use reminders to log off after a set duration.

Example: Apps like "Forest" allow users to set focus sessions, rewarding them for staying offline by growing virtual trees.

Being Mindful of Mental Health

Excessive internet use can negatively impact mental well-being. Addressing stress and anxiety related to online activities is vital.

Turn off unnecessary notifications to reduce distractions.

Seek professional help if internet addiction affects daily life.

Example: If constant notifications cause stress, turning off alerts during work hours can promote focus and calmness.

SHORT QUESTIONS

Q. 30 What are intellectual property rights?

Ans: INTELLECTUAL PROPERTY RIGHTS

Intellectual property rights are legal protections for the creations of individuals or organizations, such as books, music, inventions, or software. They ensure that creators have exclusive control over their work and can decide how it is used, shared, or sold. For example, an author who writes a novel has the right to control its publication and adaptation, preventing unauthorized reproduction or distribution.

Q. 31 What is copyright?

Ans: COPYRIGHT

Copyright is a legal right that protects original works like music, books, movies, and software, giving creators control over their use. It ensures that no one else can copy, distribute, or modify these works without permission. For instance, a filmmaker owns the copyright to their movie and can decide how it is screened or distributed.

Q. 32 What is a trademark?

Ans: TRADEMARK

A trademark is a unique symbol, logo, or slogan used to distinguish a company's products or services from competitors. It protects brand identity and prevents others from using similar marks that could confuse customers. For example, the Nike "swoosh" logo is a trademark, ensuring that only Nike can use it on their products.

Q. 33 What does a patent protect?

Ans: PATENT PROTECT

A patent protects new inventions or processes, giving inventors exclusive rights to make, use, or sell their creations for a specific period. It prevents others from copying or profiting from the invention without permission. For example, a company that invents a new type of solar panel can patent it to safeguard their innovation from competitors.

Q. 34 Why is respecting intellectual property important?

Ans: RESPECTING INTELLECTUAL PROPERTY IMPORTANT

Respecting intellectual property ensures that creators are fairly rewarded for their work and motivates innovation and creativity. Unauthorized use or copying, such as pirating movies or

software, deprives creators of their rightful income and can discourage further development. For example, buying a licensed copy of software supports the developers financially, enabling them to improve their product.

Q. 35 What is software piracy?

Ans: **SOFTWARE PIRACY**

Software piracy involves the illegal copying, distribution, or use of software without proper licensing. It violates intellectual property laws and harms developers by depriving them of revenue needed to create and update their products. For instance, downloading a paid software program without purchasing it constitutes piracy and is both unethical and illegal.

Q. 36 How does private browsing protect your privacy?

Ans: **BROWSING PROTECT YOUR PRIVACY**

Private browsing prevents your web browser from saving your search history, cookies, and personal data during a session. This helps protect sensitive information when researching online or using shared computers. For example, if you are looking up medical information, private browsing ensures that your searches are not stored or shared.

Q. 37 Why is it important to cross-check information online?

Ans: **IMPORTANT TO CROSS-CHECK INFORMATION ONLINE**

Cross-checking information ensures accuracy and reliability by verifying it against multiple credible sources. It helps avoid spreading misinformation or relying on false data. For example, if researching health advice, consulting government health websites and academic journals ensures you get accurate and trustworthy information.

Q. 38 What is internet addiction?

Ans: **INTERNET ADDICTION**

Internet addiction occurs when excessive online activity interferes with daily responsibilities and relationships. It can manifest as constant scrolling on social media, gaming for hours, or neglecting work and family. For instance, if someone spends all night online and struggles to focus during the day, they may be experiencing internet addiction.

Q. 39 What are signs of internet addiction?

Ans: **SIGNS OF INTERNET ADDICTION**

Signs of internet addiction include difficulty limiting online time, neglecting responsibilities, and feeling anxious when not connected. It may also involve avoiding offline activities. For example, a student who spends hours gaming instead of studying or spending time with family may be addicted to the internet.

Q. 40 How can you prevent internet addiction?

Ans: **PREVENT INTERNET ADDICTION**

Preventing internet addiction involves setting time limits for online activities, balancing screen time with offline hobbies, and recognizing unhealthy patterns. For example, scheduling one hour daily for social media and using the rest of the time for sports or reading can help maintain balance.

Q. 41 What is a strategy for safe online research?

Ans: **STRATEGY FOR SAFE ONLINE RESEARCH**

Safe online research includes using credible websites, avoiding suspicious links, and protecting personal data. For example, choosing websites with ".edu" or ".gov" extensions ensures reliability, and using private browsing prevents your history from being tracked.

Q. 42 What is cyberbullying?

Ans: **CYBERBULLYING**

Cyberbullying involves using digital platforms to harm or harass someone through mean messages, rumors, or posting embarrassing content. It can negatively affect mental health and self-esteem. For instance, spreading false rumors about a classmate on social media is an example of cyberbullying.

Q. 43 How can you address cyberbullying?

Ans: ADDRESS CYBERBULLYING

Addressing cyberbullying includes reporting the behavior, blocking the bully, and offering support to the victim. Social media platforms provide tools for reporting abusive content. For example, if someone is harassed on Instagram, they can block the user and report the incident to the platform.

Q. 44 Why is digital well-being important?

Ans: DIGITAL WELL-BEING IMPORTANT

Digital well-being ensures a healthy and balanced use of technology, preventing stress, addiction, and mental fatigue. For example, taking breaks during long online sessions and using screen time management tools can reduce the negative effects of excessive internet use.

Q. 45 What does responsible sharing on social media involve?

Ans: RESPONSIBLE SHARING ON SOCIAL MEDIA INVOLVE

Responsible sharing involves being cautious about what you post and adjusting privacy settings to protect personal information. For instance, setting your account to "private" ensures that only trusted followers can see your content. Sharing respectful and accurate information also fosters a positive online environment.

Q. 46 What are strategies for digital well-being?

Ans: STRATEGIES FOR DIGITAL WELL-BEING

Strategies include setting time limits for online activities, taking regular breaks, and balancing screen time with offline hobbies. For example, installing apps that track and limit screen time can help manage internet usage effectively.

Q. 47 Why is online etiquette important?

Ans: ONLINE ETIQUETTE IMPORTANT

Online etiquette fosters respectful interactions, promotes positive communication, and reduces conflicts. For example, using polite language in comments or avoiding offensive remarks can create a supportive digital community.

Q. 48 What are ".edu" websites?

Ans: EDU" WEBSITES

Websites with ".edu" domains are associated with educational institutions and are generally reliable sources for research. For example, a university's website providing academic articles is a trusted resource compared to random blogs.

Q. 49 What is the impact of software piracy?

Ans: IMPACT OF SOFTWARE PIRACY

Software piracy causes financial losses for developers, discourages innovation, and leads to legal consequences. For instance, if people download unlicensed software, the creators lose revenue needed to improve the product, which ultimately affects users as well.

MULTIPLE CHOICE QUESTIONS

59. What is the primary purpose of intellectual property rights?

- | | |
|-------------------------|--------------------------------------|
| (A) To limit creativity | (B) To protect ideas and creations |
| (C) To encourage piracy | (D) To promote free sharing of ideas |

60. What does copyright protect?

- | | |
|---|-------------------|
| (A) Company slogans | (B) Inventions |
| (C) Original works like music and books | (D) Customer data |

61. What is a trademark?

- | | |
|------------------------------------|---|
| (A) A legal right for inventions | (B) A unique symbol or slogan for a brand |
| (C) A right to copy someone's work | (D) A privacy law |

62. Which of the following is an example of a trademark?

- | | |
|---------------------|------------------------|
| (A) A novel | (B) A company logo |
| (C) A new invention | (D) A software program |

63. **What is a patent designed to protect?**
(A) Books and movies (B) New inventions or processes
(C) Brand slogans (D) User data
64. **What is an ethical responsibility regarding intellectual property?**
(A) Copying software freely
(B) Downloading movies illegally
(C) Seeking permission before using someone's work
(D) Sharing copyrighted materials
65. **What does software piracy involve?**
(A) Protecting intellectual property (B) Illegally copying or distributing software
(C) Developing new software (D) Using software legally
66. **What is the consequence of software piracy?**
(A) Supporting software developers (B) Improving digital ethics
(C) Cheating developers out of revenue (D) Enhancing software features
67. **What is the purpose of private browsing?**
(A) To save browsing history (B) To enhance search speed
(C) To protect privacy during research (D) To access private websites
68. **How can you assess the credibility of online information?**
(A) Rely on a single source (B) Avoid cross-checking
(C) Use multiple trustworthy sources (D) Trust sensational headlines
69. **What should you do to avoid internet addiction?**
(A) Spend unlimited time online (B) Set time limits for internet use
(C) Focus only on social media (D) Avoid offline activities
70. **What is a strategy for digital well-being?**
(A) Ignore mental health (B) Use apps to manage screen time
(C) Spend all day online (D) Avoid breaks during long sessions
71. **How can you avoid privacy risks during research?**
(A) Share personal data freely (B) Click on suspicious links
(C) Use private browsing modes (D) Ignore website credibility
72. **What is cyberbullying?**
(A) Respectful online interaction (B) Using the internet to harm others
(C) Following privacy guidelines (D) Reporting inappropriate behavior
73. **What should you do if you encounter cyberbullying?**
(A) Ignore it (B) Report and block the bully
(C) Join in the bullying (D) Avoid supporting the victim
74. **What does responsible social media sharing involve?**
(A) Ignoring privacy settings (B) Sharing confidential information
(C) Adjusting privacy settings to protect posts (D) Posting without thinking
75. **What is the importance of taking breaks during long internet sessions?**
(A) Increases screen time (B) Reduces mental fatigue
(C) Promotes addiction (D) Disrupts productivity
76. **What should you do to maintain respectful online interactions?**
(A) Post hurtful comments (B) Use polite language
(C) Spread rumors (D) Engage in arguments
77. **What is the first step in fostering healthy online habits?**
(A) Ignore stress caused by the internet (B) Be mindful of mental health
(C) Overuse social media apps (D) Avoid using time management tools
78. **What kind of websites are generally credible for research?**
(A) Sensational blogs (B) Websites with ".edu" domains
(C) Personal social media accounts (D) Unverified forums

11.7 IMPACT OF COMPUTING ON SOCIETY**LONG QUESTIONS**

Q.47 Discuss the influence of computing on global trade, communication, and cultural evolution.

Ans: Computing has had a transformative impact on global trade, communication, and cultural evolution, reshaping how the world operates in numerous ways. Here's how:

Global Trade:

Computing systems have significantly improved global trade by making transactions faster and more efficient. Online platforms like Amazon, AliExpress, and Daraz facilitate cross-border shopping, allowing consumers to buy products from different countries easily. Businesses use computers for managing inventories, processing payments, and tracking shipments. These systems help to reduce costs, streamline operations, and expand market reach. For instance, a company in one country can sell products to customers around the world without needing a physical store in each location. This globalization of commerce has also led to the rise of new industries such as e-commerce and digital marketing.

Communication:

Computing technology has revolutionized communication by allowing instant global connections. Email, messaging apps, and social media platforms like Facebook, WhatsApp, and Instagram enable real-time exchanges between individuals and organizations across the globe. Video conferencing tools, such as Zoom, make it possible to hold virtual meetings, making global collaboration easier and more cost-effective. Furthermore, communication barriers like geographical distance and time zone differences have been significantly reduced, enabling quicker decision-making and international cooperation. This has not only enhanced personal connections but also streamlined business processes.

Cultural Evolution:

Computing has also played a crucial role in the cultural evolution by enabling the rapid sharing and spread of cultures. Platforms like YouTube, Instagram, and TikTok allow individuals from different cultures to share their traditions, art, and ideas with a global audience. For example, a traditional dance from one country can quickly gain popularity and influence in others through viral videos. This interconnectedness leads to greater cultural exchange, breaking down cultural barriers and promoting a more inclusive world. Moreover, computing has made it easier for people to access diverse forms of media, literature, and music from around the world, further enriching cultural experiences.

Q.48 Explain the benefits and risks of computing advancements, particularly in social networking and misinformation.

Ans: Computing advancements, especially in social networking and the proliferation of information, bring both numerous benefits and serious risks. Here's an in-depth explanation of both aspects:

1. Benefits of Social Networking:

Social networking platforms have fundamentally changed how people connect, interact, and share information. The key benefits of social networking include:

Connection and Communication: Social networks, such as Facebook, Twitter, and LinkedIn, allow people to stay in touch with family and friends across the globe, breaking down geographical barriers. Instant messaging, status updates, and group discussions help maintain relationships and facilitate communication.

Information Sharing and Collaboration: These platforms enable users to share ideas, opinions, and knowledge quickly. For instance, platforms like LinkedIn help professionals build networks, while Twitter enables the rapid dissemination of news and updates. Social media has also become a powerful tool for businesses to interact with customers and promote their products.

Community Building: Social media platforms foster the creation of interest-based communities. These communities can provide support, share resources, and collaborate on projects, further strengthening social ties and collective efforts.

2. **Risks of Social Networking:**
While social networking brings several benefits, it also comes with notable risks, including:
Cyberbullying: The anonymity that online platforms provide can lead to harmful behaviors like cyberbullying. This issue, which involves using the internet to harm or harass others, can have serious psychological effects on victims.
Privacy Concerns: The sharing of personal information on social networking sites can lead to privacy breaches. Many platforms collect vast amounts of data, which may be misused by third parties for purposes like targeted advertising or even identity theft.
Addiction: Overuse of social networking platforms can lead to internet addiction. This can interfere with daily activities, productivity, and real-world social interactions, ultimately impacting mental health.
3. **Misinformation Risks:**
One of the significant risks associated with the rise of computing and social media is the spread of misinformation. Misinformation refers to false or misleading information that can spread quickly across social networks. The consequences of misinformation include:
Public Harm: False health information, like unproven medical treatments, can cause harm to people who believe and act on it. For example, during the COVID-19 pandemic, misinformation about treatments or vaccines contributed to confusion and distrust.
Erosion of Trust: Misinformation erodes public trust in reliable sources, such as news outlets and scientific communities. When people are unable to distinguish between factual and false information, it undermines the credibility of authoritative sources.
Polarization: Misinformation can exacerbate social divisions. False narratives, especially political ones, can lead to the spread of hatred, division, and confusion, often leading to real-world consequences such as protests or violence.
4. **Balancing Privacy, Security, and Usability:**
A key trade-off in computing advancements lies in balancing privacy, security, and usability. High-security measures, such as encryption and multi-factor authentication, can protect user data and privacy but may also make systems less user-friendly. This trade-off poses challenges for developers, who must design systems that ensure user protection without compromising convenience. For example, requiring complex passwords or additional verification steps might enhance security but can also frustrate users who seek quick and seamless access to their accounts.

SHORT QUESTIONS

- **How does computing technology influence society?**
Ans: COMPUTING TECHNOLOGY INFLUENCE SOCIETY
Computing technology significantly influences how we live, work, and communicate. It enables instant global communication, facilitates online transactions, and creates new industries like software development. However, it also introduces challenges, such as ethical dilemmas and cyberbullying. For example, social media helps us connect but can lead to misinformation if not managed responsibly.
- **What are the ethical impacts of computing?**
Ans: ETHICAL IMPACTS OF COMPUTING
The ethical impacts of computing involve respecting intellectual property, maintaining privacy, and ensuring fair usage. For instance, downloading music without permission violates copyright laws, which is unethical. Ethical computing encourages transparency and accountability in the use of technology.
- **How does computing affect societal behavior?**
Ans: COMPUTING AFFECT SOCIETAL BEHAVIOR
Computing reshapes how people interact, often through social media platforms like Facebook and Instagram. While it fosters global connections, it also introduces challenges like cyberbullying

and reduced face-to-face communication. For instance, constant online engagement might hinder real-world relationships.

- **Explain the economic impact of computing.**

Ans: **ECONOMIC IMPACT OF COMPUTING**

Computing drives economic growth by creating new industries such as e-commerce and digital marketing. However, it also leads to job displacement due to automation. For example, online shopping platforms like Amazon reduce the need for physical retail staff but create logistics and IT roles.

- **What is the role of computing in global trade?**

Ans: **ROLE OF COMPUTING IN GLOBAL TRADE**

Computing facilitates global trade by simplifying transactions, managing inventory, and tracking shipments. Platforms like AliExpress enable cross-border shopping, allowing consumers to buy products from other countries with ease.

- **What are the benefits and risks of social networking?**

Ans: **BENEFITS AND RISKS OF SOCIAL NETWORKING**

Social networking connects people worldwide, enabling quick communication and information sharing. However, it also spreads misinformation, which can mislead users. For example, false news about health risks can cause unnecessary panic if not verified.

- **How does cultural evolution relate to computing?**

Ans: **CULTURAL EVOLUTION RELATE TO COMPUTING**

Computing aids cultural evolution by enabling the global sharing of traditions and ideas through platforms like YouTube. For instance, a cooking video can introduce one culture's cuisine to a worldwide audience, promoting cultural exchange.

- **What are trade-offs between privacy and usability in computing systems?**

Ans: **TRADE-OFFS BETWEEN PRIVACY AND USABILITY IN COMPUTING SYSTEMS**

Enhanced privacy measures, such as strong passwords or encryption, may reduce usability by making systems more complex. For example, two-factor authentication improves security but adds steps to the login process, potentially inconveniencing users.

- **How does computing address global communication challenges?**

Ans: **COMPUTING ADDRESS GLOBAL COMMUNICATION CHALLENGES**

Computing solves communication barriers with tools like video conferencing, instant messaging, and email. For instance, businesses can hold international meetings using Zoom, enabling collaboration across different time zones.

- **Why is combating misinformation important?**

Ans: **COMBATING MISINFORMATION IMPORTANT**

Misinformation can lead to confusion and harmful decisions. Verifying facts from reliable sources prevents the spread of false narratives. For example, debunking fake health claims on social media ensures public safety and trust in accurate information.

MULTIPLE CHOICE QUESTIONS

Q. 2 Which aspect of society is most impacted by computing technology?

- (A) Environment
- (B) Cultural practices
- (C) Societal behavior
- (D) All of the above

Q. 3 What does computing raise in terms of ethics?

- (A) Productivity issues
- (B) Legal concerns
- (C) Ethical questions about usage
- (D) None of the above

Q. 4 What is a legal impact of computing?

- (A) Improved productivity
- (B) Enhanced creativity
- (C) Privacy laws and regulations
- (D) Global cultural exchange

Q. 5 Which is a societal impact of computing?

- (A) Increased energy use
- (B) Cyberbullying

- (C) Reduced connectivity (D) Global trade reduction
- Q. 6 How has computing affected economic practices?**
(A) It has created new industries. (B) It has slowed down global trade.
(C) It has limited access to technology. (D) It has reduced automation.
- Q. 7 What role does computing play in global trade?**
(A) It complicates transactions. (B) It enables efficient inventory management.
(C) It limits international purchases. (D) It prevents fraud entirely.
- Q. 8 What is one benefit of social networking platforms?**
(A) They eliminate misinformation. (B) They help people stay connected.
(C) They replace traditional media. (D) They reduce online communication.
- Q. 9 Which risk is associated with social media platforms?**
(A) Spread of false information (B) Reduced global trade
(C) Limited cultural interaction (D) Reduced system usability
- Q. 10 What is a trade-off between privacy and usability?**
(A) Strong security reduces time consumption.
(B) Privacy measures can make systems harder to use.
(C) Usability always prioritizes privacy.
(D) Trade-offs only apply to security, not usability.
- Q. 11 What is a cultural benefit of computing?**
(A) It prevents traditional practices. (B) It spreads cultures globally.
(C) It limits cultural communication. (D) It replaces cultural identity.
- Q. 12 What do privacy laws aim to protect?**
(A) Economic interests (B) Personal information
(C) Social platforms (D) Cultural exchange
- Q. 13 Which is an example of misinformation on social media?**
(A) Verified health facts (B) False news stories
(C) Accurate product reviews (D) Secure online transactions
- Q. 14 What does two-factor authentication enhance?**
(A) Usability (B) Security
(C) Privacy (D) Connectivity
- Q. 15 What is a global communication benefit of computing?**
(A) It reduces collaboration. (B) It enables instant messaging.
(C) It limits access to emails. (D) It makes video calls redundant.
- Q. 16 How does automation affect traditional jobs?**
(A) It creates more manual work. (B) It replaces some roles.
(C) It limits technological growth. (D) It only affects software developers.

SUMMARY

- Safe and responsible computer usage means knowing how to protect our personal information, making wise choices about the hardware and software we use, and ensuring that our online behavior is respectful and ethical.
- Responsible computer usage means protecting ourselves and others when using computers.
- Safe operation of digital platforms and devices, mean using them in a way that protects you from harm and avoids any unwanted issues.
- Using digital platforms securely means taking extra steps to protect your information and ensuring that your online activities do not put you or others at risk.
- Privacy settings and data security measures are essential tools that help protect your personal information while using digital platforms.
- Privacy laws are rules set by the government to protect our personal information. These laws ensure that companies and organizations handle our data responsibly.

- Ethical guidelines for data usage involve ensuring that data is used for the purpose it was intended and that it benefits the person who provided it.
- Intellectual property rights are important because they protect the creations and ideas of individuals and organizations.
- Copyright is a legal right that gives creators control over their original works, such as music, books, movies, and software.
- Trademarks are symbols, names, or slogans used by companies to distinguish their products or services from others.
- Patents protect new inventions or processes, giving the inventor exclusive rights to make, use, or sell the invention for a certain period.
- Software piracy is the illegal copying, distribution, or use of software.

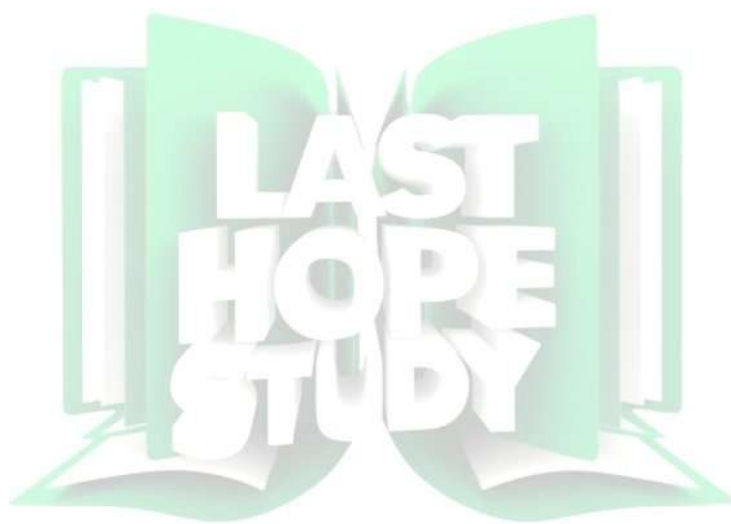
EXERCISE**MULTIPLE CHOICE QUESTIONS**

89. **Why is it important to use computers safely and responsibly?**
(A) To ensure we can use them more frequently
(B) To protect our personal information and make wise choices about hardware and software
(C) To make the computer run faster
(D) To avoid paying for software
90. **What does "responsible computer usage" include?**
(A) Choosing the most expensive hardware
(B) Sharing your passwords with friends
(C) Being cautious about what you share online and protecting yourself and others
(D) Ignoring software updates
91. **What should you check to ensure hardware and software compatibility?**
(A) The color of the hardware
(B) The system requirements on software packages and match them with your computer's specifications
(C) The price of the hardware
(D) The brand of the hardware
92. **Why is it important to use strong, unique passwords?**
(A) To make your accounts easy to hack
(B) To help others guess your password
(C) To make it harder for someone to guess your password and access your accounts
(D) To avoid installing software updates
93. **What is one reason to avoid clicking on unknown links or downloading files from untrusted sources?**
(A) They might contain helpful software
(B) They might contain malware that can harm your device or steal your information
(C) They are usually cheaper
(D) They help your device run faster
94. **What does Two-Factor Authentication (2FA) do?**
(A) It makes your password easier to guess
(B) It adds an extra layer of security by requiring a second form of verification
(C) It removes the need for a password
(D) It reduces the need for software updates
95. **Why should you be cautious when using public Wi-Fi for sensitive transactions?**
(A) Public Wi-Fi is usually faster
(B) Public Wi-Fi networks are often less secure
(C) Public Wi-Fi is free
(D) Public Wi-Fi always provides encryption
96. **What is an important aspect of responsible use of social media?**

- (A) Sharing personal information like your home address
(B) Posting photos without considering privacy settings
(C) Being respectful and avoiding sharing sensitive information publicly
(D) Ignoring privacy settings
97. **What should you do if you receive an email from an unknown sender asking for personal information?**
(A) Provide the information requested (B) Forward the email to your friends
(C) Ignore or delete the email (D) Open the email and click on any links
98. **Why is it important to regularly review your account activity?**
(A) To update your contact information
(B) To look for unusual activity and ensure your accounts are secure
(C) To check the number of friends you have
(D) To download new applications
99. **What is the purpose of privacy settings on digital platforms?**
(A) To make your posts public
(B) To control who can see your information and interact with you online
(C) To increase the number of followers
(D) To automatically share your information
100. **What should you do to ensure data security?**
(A) Use the same password for all accounts
(B) Share your passwords with friends
(C) Use strong, unique passwords and enable two-factor authentication
(D) Avoid using any security measures
101. **What is a key aspect of data ethics?**
(A) Using data in any way you like
(B) Transparency, respect for privacy, and accountability in data usage
(C) Collecting as much data as possible
(D) Ignoring data security
102. **What is software piracy?**
(A) Sharing software legally with friends
(B) The illegal copying, distribution, or use of software
(C) Buying software from an official source
(D) Updating software regularly
103. **How can you verify the credibility of information found online?**
(A) By checking the number of ads on the website
(B) By using multiple reputable sources and checking the author's credentials
(C) By looking at the website's design
(D) By the website's popularity

SHORT QUESTIONS

- Q. 67 What is the importance of using computers safely and responsibly?**
Ans: Using computers safely and responsibly is essential for protecting personal information, maintaining respectful online behavior, and ensuring the safety and efficiency of hardware and software. This practice helps in enjoying technology while avoiding risks.
- Q. 68 How does choosing the right hardware and software affect your computer usage?**
Ans: Choosing the right hardware and software impacts safety, efficiency, and compatibility. Properly matched components reduce risks, improve task completion speed, and enhance overall user experience.
- Q. 69 Why is it important to use antivirus software on your computer?**
Ans: Antivirus software protects your system from malware, viruses, and other threats. It ensures data integrity, prevents unauthorized access, and improves the security of your digital environment.



Q. 70 What are some examples of good practices when selecting hardware and software?

Ans: Good practices include:

Verifying compatibility with your system.

Researching the reliability of hardware and software vendors.

Regularly updating software to address vulnerabilities.

Q. 71 How can choosing compatible hardware and software enhance your computer experience?

Ans: Compatible hardware and software ensure smooth operation, reduce conflicts, and enable optimal performance. They also minimize frustration from crashes or incompatibility issues.

Q. 72 Why should you create strong, unique passwords for your accounts?

Ans: Strong, unique passwords reduce the risk of unauthorized access. They protect your accounts from hacking and safeguard sensitive data. Examples of strong passwords include a mix of letters, numbers, and symbols.

Q. 73 What is the purpose of regular software updates?

Ans: Software updates provide critical security fixes, enhance functionality, and ensure compatibility with other systems. They prevent vulnerabilities that hackers might exploit.

Q. 74 How can you protect yourself from harmful links and downloads?

Ans: Avoid clicking on unknown links and downloading files from untrusted sources. Use antivirus software to scan files before opening them.

Q. 75 What is Two-Factor Authentication (2FA), and why is it useful?

Ans: 2FA adds an additional layer of security by requiring a second form of verification, such as a code sent to your phone. This makes it harder for unauthorized users to access your accounts.

Q. 76 Why is it a good idea to avoid using public Wi-Fi for sensitive transactions?

Ans: Public Wi-Fi is often insecure, making it vulnerable to hackers who can intercept sensitive data. Avoid using it for transactions like online banking.

Q. 77 How can you verify if an email or message is a scam?

Ans: To identify scams, check for generic greetings, spelling errors, suspicious links, and unsolicited requests for personal information. Always verify the sender's identity and avoid clicking on unknown links.

Q. 78 Why is it important to be careful about what you share on social media?

Ans: Sharing too much on social media can expose you to identity theft or scams. It's important to adjust privacy settings and avoid posting personal details like your address, phone number, or financial information.

Q. 79 What should you do if you receive an email from an unknown sender asking for personal information?

Ans: Ignore or delete the email, mark it as spam, and never provide any personal information. Verify its authenticity by contacting the company directly if needed.

Q. 80 What is the purpose of privacy laws regarding your personal information?

Ans: Privacy laws protect your personal data by ensuring organizations collect, use, and store it responsibly. They also grant individuals the right to control their information and take legal action against misuse.

Q. 81 How do privacy laws protect you from unauthorized access to your data?

Ans: Privacy laws mandate strong security measures like encryption and prohibit unauthorized access to personal data. Companies can face penalties for failing to protect user information.

Q. 82 What is the difference between copyright, trademarks, and patents?

Ans: Copyright: Protects original works like books, music, and software.

Trademarks: Safeguard brand names, logos, and slogans.

Patents: Cover new inventions and processes, granting exclusive rights to inventors.

Q. 83 Why is it important to respect intellectual property rights?

Ans: Respecting intellectual property rights encourages innovation, ensures fair compensation for creators, and avoids legal consequences like penalties for violations.

Q. 84 What is software piracy, and why is it harmful?

Ans: Software piracy involves the unauthorized copying or use of software. It harms developers financially, increases cybersecurity risks, and stifles innovation in the software industry.

Q. 85 How can you identify reliable sources when researching online?

Ans: Use credible websites, cross-check information across multiple sources, and prioritize websites ending in .edu or .org. Avoid sources with sensational headlines.

Q. 86 What is one way to protect your privacy during online research?

Ans: Use private browsing modes to avoid saving your browsing history and avoid entering personal details on unfamiliar websites.

Q. 87 What are some signs that you might be developing an internet addiction?

Ans: Signs include neglecting responsibilities, excessive screen time, feeling anxious without internet access, and prioritizing online activities over real-life interactions.

LONG QUESTIONS

1. Discuss the importance of responsible computer usage in today's digital world. Explain how selecting the right hardware and software can affect safety, efficiency, and compatibility in computer use.
See Topic 11.1
2. Describe the steps you should take to ensure the safe operation of digital platforms and devices.
See Topic 11.2
3. Explain the concept of data ethics and its importance in handling personal and sensitive information. Discuss the principles of transparency, respect for privacy, and accountability.
See Topic 11.3
4. Analyze the impact of privacy laws on protecting personal information in the digital age. How do laws like the Personal Data Protection Bill in Pakistan help safeguard user data?
See Topic 11.5
5. Discuss the different types of intellectual property rights, including copyright, trademarks, and patents.
See Topic 11.4
6. Describe the ethical and legal responsibilities related to intellectual property rights. What are the consequences of violating these rights, such as through software piracy or unauthorized use of copyrighted material?
See Topic 11.4
7. Outline effective techniques for conducting safe and credible online research. How can users evaluate the reliability of sources and avoid privacy risks during their research?
See Topic 11.6
8. Discuss the concept of internet addiction and its potential impact on individuals. How can recognizing the signs of addiction, setting time limits, and finding offline activities help promote balanced internet usage?
See Topic 11.6

ANSWER KEYS**TOPIC 11.1 RESPONSIBLE COMPUTER USAGE 11.2 SAFE AND SECURE OPERATIONS OF DIGITAL PLATFORMS**

1	C	2	B	3	B	4	B	5	B
6	C	7	B	8	B	9	C	10	B
11	B	12	B	13	B	14	B	15	B

TOPIC 11.3 BEST PRACTICES IN ONLINE BEHAVIOUR

1	B	2	B	3	B	4	B	5	B
6	B	7	B	8	B	9	A	10	B
11	B	12	C	13	B	14	B	15	C

TOPIC 11.4 LEGAL AND ETHICAL FRAMEWORKS

1	B	2	C	3	B	4	C	5	A
6	A	7	A	8	B	9	C	10	B
11	B	12	B	13	B	14	B	15	B

TOPIC 11.5 INTELLECTUAL PROPERTY RIGHTS

1	B	2	C	3	B	4	B	5	B
6	C	7	B	8	C	9	C	10	C
11	B	12	B	13	C	14	B	15	B
16	C	17	B	18	B	19	B	20	B

TOPIC 11.6 RESPONSIBLE INTERNET USE 11.7 IMPACT OF COMPUTING ON SOCIETY

1	D	2	C	3	C	4	B	5	A
6	B	7	B	8	A	9	B	10	B
11	B	12	B	13	B	14	B	15	B

TEXTBOOK EXERCISE MCQs

1	B	2	C	3	B	4	C	5	B
6	B	7	B	8	C	9	C	10	B
11	B	12	C	13	B	14	B	15	B