

Chapter 9

Cybersecurity and Safe Digital Collaboration

Student Learning Outcomes:

By the end of this chapter, students will be able to:

- Identify and apply safe practices when collaborating on digital or online platforms.
- Understand of common types of cybersecurity problems and topics such as 2FA, biometric verification, and secure techniques for transmitting data.
- Collaborate on creation of digital applications and understand strategies to design for equity and equal access to information.
- Explore digital entrepreneurship concepts and develop simple technology-based business ideas using digital platforms and collaborative tools.

Introduction

In this chapter, students will explore how technology supports safe, secure, and responsible participation in the digital world. They will learn about online safety, cybersecurity, data protection, privacy settings, and secure collaboration using modern digital platforms. The chapter also introduces digital entrepreneurship, innovation, and the skills needed to identify business opportunities and solve real-world problems through technology. Students will explore ethical, legal, social, and environmental aspects of computing, including intellectual property, data privacy, cybersecurity laws, and sustainable computing practices. They will also learn the importance of teamwork, accessibility, digital communication, and responsible use of technology in personal, educational, and professional settings (as shown in Figure 9.1). By the end, students will understand how to use technology safely, responsibly, ethically, effectively, and creatively in daily life and future careers.

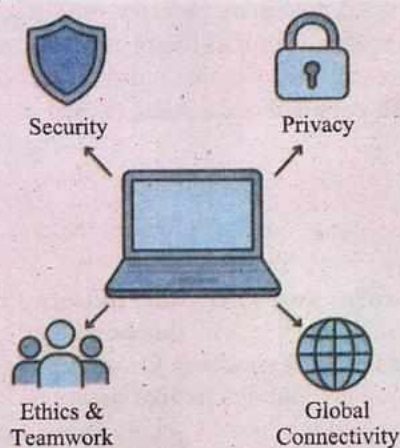


Figure 9.1: Cybersecurity, Ethics, and Digital Collaboration in Today's Connected World



9.1 Safe and Responsible Digital Practices

This section explains how to use technology wisely and protect personal information while working online. Students learn the importance of safe habits, like using strong passwords, keeping software updated, and avoiding unsafe websites (as shown in Figure 9.2). Practicing responsible digital behavior helps prevent data loss, hacking, and identity theft. By following safety rules, users can enjoy the benefits of technology without unnecessary risks. These habits build trust and create a secure digital environment for everyone.



Figure 9.2: Safe Digital Practices

? DO YOU KNOW?

A strong password with 12 characters can take millions of years for a computer to crack, but a weak one can be cracked in seconds.

Importance of Online Safety

Online safety means protecting yourself and your information while using the internet. It includes being careful about what you share, where you click, and how you store your data. Students learn that online actions leave digital footprints that can be tracked. By understanding the importance of safety, users can avoid scams, viruses, and cyber threats. Staying alert and cautious online helps keep both personal and school-related data secure.



TIDBIT

Understanding threats and preventive measures, reduces the chance of cybercrime.

Understanding Strong Passwords and Their Role in Data Protection

A strong password is a combination of letters, numbers, and symbols that helps protect your accounts from hackers. Using unique passwords for different accounts reduces the chance of being hacked. It's best to avoid personal details like names or birthdays. Passwords should be changed regularly and not shared with others. A secure password acts as the first line of defense in protecting important files and data online.



Risks of Downloading Suspicious Software and Unsafe Browsing Habits

Downloading programs or files from unknown websites can harm your computer or steal your information. Some downloads hide viruses or spyware that collect data without permission. Unsafe browsing, such as visiting fake websites or clicking unknown links, can also lead to scams or identity theft. It is important to check sources before downloading and use antivirus tools for extra protection. Safe browsing habits help keep both devices and data secure.

Software Maintenance and Updates

Software maintenance means keeping programs and applications in good working condition by updating them regularly. Updates often fix errors, improve performance, and add new features that make software safer to use. Students learn that software companies release updates to close security gaps that hackers might exploit. Ignoring updates can lead to slow systems, crashes, or data theft. Regular maintenance keeps computers reliable, efficient, and protected from cyber threats.

When software is not updated, it becomes an easy target for hackers. Older versions may have security holes that allow unauthorized access to files or personal data. Outdated software can also cause compatibility issues with new systems or tools. Using such programs increases the risk of malware infections and data breaches. Regularly updating software reduces these risks and keeps your system safe and dependable.



CLASS ACTIVITY

Students compare features of updated vs outdated software and discuss how old versions can be attacked.

Privacy and Security Settings

Privacy and security settings help users control how their personal information is used and shared online. These settings are found in most apps, websites, and digital platforms. Students learn how to adjust them to protect personal data such as location, contacts, and browsing history. Managing privacy helps prevent misuse of information by unwanted sources or advertisers. Understanding and using these settings keeps online activities more private and secure. For example, on Instagram, users can make their account private so that only approved followers can see their posts. They can also turn off location sharing to protect their privacy and enable two-factor authentication for extra account security.

Reading and Managing Privacy Policies

Privacy policies explain how a website or app collects, stores, and uses your information. It is important to read them carefully before creating an account or agreeing to terms. By reviewing these policies, users can decide whether to share personal data or not. Students learn to check what kind of data is being collected and for what purpose. Managing privacy responsibly ensures that personal details are not shared without permission. A privacy policy tells users how their data is collected, used, stored, and shared. For example, when signing up for any social platform, the privacy policy explains what type of data may be collected, such as name, email address, location, browsing activity, and app usage. It may also explain whether this data is shared with advertisers or third-party services.

TIDBIT

Regularly reviewing settings ensures protection as platforms update their features.



Customizing Privacy and Security Settings for Online Platforms

Most online platforms allow users to change their privacy and security settings based on their comfort level. These settings can control who sees your posts, who can contact you, and how data is used. Turning on features like two-factor authentication and limiting app permissions increases safety. The user should regularly review and update their settings as platforms often change their privacy rules. Customizing these options gives users more control over their digital presence and protection. For example, on WhatsApp, users can choose who can see their profile photo, such as everyone, only contacts, or nobody. They can also disable read receipts, commonly known as blue ticks, so that others cannot see whether their messages have been read.

Safe Online Collaboration

Online collaboration allows people to work together using digital tools from any location. It is important to use secure platforms and follow safety rules when sharing files or communicating online. Students learn to work responsibly in virtual groups while protecting personal and school data. Safe collaboration builds trust and ensures productive and respectful teamwork. For example, while using Google Docs for group work, students should share the document only with trusted classmates. They should also set the permission to “View only” instead of “Edit” if others only need to read the document. This helps protect the document from unwanted changes and keeps the work secure.

Identifying Secure Collaboration Platforms (e.g., Google Workspace, MS Teams)

Secure collaboration platforms such as Google Workspace and Microsoft Teams provide protected environments for group work. These platforms use features like encrypted communication and access controls to safeguard data. Students can share documents, attend meetings, and communicate safely. Choosing trusted and approved platforms helps protect information and reduces cyber risks. For example, students can use Google Workspace for school projects by sharing a project file only with selected classmates through restricted access. They can also use Google Meet for secure online classes, where only authorized participants are allowed to join. These features help students collaborate safely while protecting their schoolwork and personal information.

Practicing Digital Etiquette and Responsible Communication

Digital etiquette means communicating politely, respectfully, and clearly in online environments. It includes using appropriate language, respecting others' opinions, and avoiding misuse of communication tools. Students should not share private information or behave disrespectfully during online interactions. Responsible communication promotes teamwork and helps maintain a positive and professional digital environment. For example, in a class group chat, students should respect others' opinions during discussions. They should avoid sending spam messages, unrelated memes, or jokes during serious academic discussions. This helps keep the group useful, respectful, and focused on learning.

9.2 Cybersecurity Awareness and Threat Management

Cybersecurity awareness means understanding how to protect computers, networks, and data from attacks. As people rely more on technology, cyber threats have become common in daily



life. Hackers use tricks and harmful software to steal information or damage systems. Being aware of these dangers helps users stay alert and act safely online. Knowing how to detect, prevent, and respond to threats keeps personal and organizational data secure. For example, users should install antivirus software to protect their computers from malware and other security threats. They should also avoid using public Wi-Fi for online banking or other sensitive work because public networks may not be secure.

TIDBIT

Avoid offensive language, spam, and sharing confidential information.

Understanding Cyber Threats

Cyber threats are actions or programs that target computers and networks to cause harm. These include stealing information, damaging systems, or interrupting online services. Understanding how threats work helps users recognize early warning signs. Most attacks can be avoided by safe browsing, using antivirus software, and being cautious with emails and links. Recognizing threats is the first step toward protecting digital systems.

DO YOU KNOW?

Phishing is among the most common attacks.

Common Types of Cyberattacks

There are different kinds of cyber threats. A **virus** spreads through infected files and can damage or delete data. **Phishing** tries to trick people into sharing passwords or personal details through fake emails or websites. **Ransomware** locks data and demands payment to unlock it, while spyware secretly collects user information. **Distributed Denial of Service (DDoS)** attacks overload websites, making them crash.

How Cyberattacks Affect Individuals and Organizations

Cyberattacks can cause serious damage to both individuals and organizations. People may lose personal files, passwords, or money, while companies may face data breaches and loss of customer trust. Attacks can stop business operations, harm reputations, and lead to financial losses. Even schools and hospitals can be affected by cyber incidents.

Security Tools and Techniques

Security tools and techniques help protect computers and networks from online threats. They make it harder for hackers or malicious software to access important information. These tools include authentication systems, firewalls, and antivirus programs that check and block harmful activities. Using them properly keeps personal data safe and reduces the chances of cyberattacks. Every computer user should understand and apply these tools to maintain digital safety.



Two-Factor Authentication (2FA)

Two-Factor Authentication (2FA) is a security method that requires two forms of verification before allowing access to an account. For example, after entering a password, the user may receive a code on their phone or email to confirm their identity. This extra step makes it much harder for hackers to break in.

Biometric Verification

Biometric verification uses physical features such as fingerprints, face scans, or voice patterns to verify identity. Biometrics add strong layers of protection to keep accounts and personal data safe.



CLASS ACTIVITY

Students simulate logging into an account with a second step (code from teacher) to understand how 2FA works.

Use of Firewalls, Intrusion Detection Systems (IDS), and Antivirus Tools

A firewall acts as a barrier between a computer and the internet, allowing safe data to pass while blocking harmful traffic. Intrusion Detection Systems (IDS) monitor networks for suspicious activities and alert users about possible threats. Antivirus software scans files and removes viruses or malware before they cause damage. Together, these tools form a powerful defense against cyberattacks. Using them regularly ensures that computers and networks remain protected and run smoothly.

Data Protection and Cryptography

Data protection means keeping digital information safe from unauthorized access, loss, or damage. It ensures that only the right people can view or use the data.



TIDBIT

Secure storage and transmission prevent unauthorized access and breaches.

Cryptography is the science of securing information so that only authorized users can understand it. It consists of two core concepts such as encryption and decryption. Encryption changes readable data into coded text using a specific key, while decryption converts it back into its original form when needed. For example, when sending a message online, encryption makes it unreadable to anyone who tries to intercept it. This process ensures that information remains private during transmission. Cryptography is widely used in secure websites, online banking, and messaging apps.

Secure Methods for Transmitting and Storing Data

Data must be protected not only when stored on a computer but also when sent over the internet.



Secure methods such as encrypted connections (like HTTPS) keep information safe during transmission. Cloud storage services also use encryption to prevent unauthorized access to saved files. Regular backups help protect data from loss caused by system failure or attacks. Following secure storage and transfer methods ensures that important data remains safe and reliable.

Detecting and Preventing Intrusions

Detecting and preventing intrusions means identifying and stopping unauthorized access to a computer or network. Cyber intrusions can occur when hackers exploit weaknesses to steal data or damage systems. Monitoring tools and security software help track unusual activity that might indicate an attack. Students learn how early detection prevents major losses and keeps systems running safely. Staying alert and updating security measures are key steps to maintaining protection against intrusions.



CLASS ACTIVITY

Students look at sample system logs or screenshots to find suspicious actions.

Identifying Vulnerabilities and Suspicious Activities

Vulnerabilities are weaknesses in software, hardware, or user behavior that hackers can exploit. Suspicious activities may include unexpected system slowdowns, unknown programs running, or strange network traffic. Regularly checking system logs and using scanning tools can help find these warning signs. Recognizing patterns of unusual behavior allows users to take quick action. Identifying and fixing vulnerabilities early reduces the chance of successful attacks.

Applying Troubleshooting and Preventive Measures

When a security issue is found, troubleshooting helps determine its cause and how to fix it. Preventive measures include installing firewalls, antiviruses and anti-malware, updating software, changing passwords, or removing harmful files. In some cases, restoring data from backups may be necessary. Documenting the problem and the steps taken helps prevent it from happening again.

9.3 Digital Collaboration and Equity in Computing

Digital collaboration means using technology to work together on shared tasks, projects, or ideas. It allows people to connect and contribute from different places using the internet. Students learn how teamwork, communication, and responsibility help achieve goals more efficiently in digital spaces (as shown in Figure 9.3).

Equity in computing ensures that everyone, regardless of background or ability, can participate and access digital resources equally. Combining collaboration with fairness helps create inclusive and effective learning and working environments.



Figure 9.3: Digital Collaboration

Working Together Online

Working together online allows teams to share ideas, exchange feedback, and complete tasks without being in the same location. It promotes cooperation and creativity through shared access to documents, discussions, and resources. Students understand that clear communication and mutual respect are key to successful online teamwork. Learning to collaborate digitally prepares them for modern workplaces where remote work is common. Online teamwork encourages problem solving and builds essential interpersonal skills.



DO YOU KNOW?

Teams that communicate clearly finish tasks faster and make fewer mistakes

Importance of Teamwork and Communication in Digital Environments

Teamwork in digital environments requires clear communication and trust among team members. When everyone contributes ideas and listens to others, projects run smoothly. Effective communication prevents misunderstandings and ensures that all members stay informed about progress. Tools like group chats, emails, and video calls help teams stay connected. Good teamwork encourages creativity, cooperation, and shared responsibility in achieving goals.

Tools and Platforms for Real-Time Collaboration

Real-time collaboration tools allow multiple users to work on the same project at the same time. Platforms such as Google Workspace, Microsoft Teams, and Zoom make sharing documents, chatting, and meeting online easier. These tools help teams organize tasks, edit files together, and stay updated instantly. Real-time collaboration saves time and reduces errors by keeping everyone aligned. Using these platforms efficiently helps teams work faster and more effectively in digital settings.

Designing for Equity and Accessibility

Designing for equity and accessibility ensures that technology can be used by everyone, including people with different abilities and backgrounds.



Equal access means that every person should have the same opportunity to use technology and the internet. This includes access to reliable devices, internet connections, and digital skills. Some people may face challenges such as disabilities, language barriers, or lack of resources. Understanding these issues helps developers and organizations design solutions that reach everyone. Equal access ensures that no one is left behind in the digital world. Accessible design; benefits people with disabilities improves usability for everyone.



CLASS ACTIVITY

Groups complete a small task, such as planning a poster, while practicing clear online-style messaging.

Creating Inclusive Applications for Diverse Users

Inclusive applications are designed to meet the needs of different types of users. This can include adding features such as screen readers for the visually impaired, subtitles for videos, or multiple language options. Simple layouts and clear text also make apps easier to use for beginners. Developers should test their designs with a variety of users to ensure accessibility for all. Creating inclusive digital tools supports equality and improves the overall user experience.

Strategies for Effective Collaboration

Effective collaboration helps teams work smoothly and complete tasks successfully. Teamwork becomes stronger when everyone understands their responsibilities and communicates clearly. Planning, organizing, and sharing ideas allow group projects to move forward without confusion. Collaboration also teaches us how to respect different opinions and work toward a common goal. The following are common strategies for effective collaboration.



TDBIT

Clear roles, task management, and goal setting improve teamwork efficiency.

Assigning Roles

Clear roles help each team member know exactly what they need to do. One person might handle research, another might organize information, while someone else prepares the final presentation.

Managing Tasks

Managing tasks by creating checklists or timelines helps the team stay on track and avoid delays.

Setting Team Goals

Setting shared goals gives everyone a direction to work toward and encourages cooperation. When roles and goals are clear, teamwork becomes much easier and more efficient.



Reflecting on Collaborative Experiences

After completing a project, it is helpful for students to think about what went well and what could be improved. Reflecting allows team members to identify strengths, such as good communication, and weaknesses, such as missed deadlines.

Discussion to Improve Teamwork

Discussing these experiences helps students learn from mistakes and become better team players. Reflection also encourages respect and understanding among group members. Over time, this practice leads to stronger teamwork and more successful collaborations.

9.4 Digital Entrepreneurship and Innovation

Digital entrepreneurship is the use of technology and online platforms to create, manage, and grow business ideas. It helps individuals solve real-world problems through innovative digital solutions. Entrepreneurs use social media, e-commerce websites, and freelancing platforms to reach customers globally. Innovation plays a key role in developing new products and services that meet changing market needs. This field provides opportunities for students to turn creative ideas into successful digital businesses.

DO YOU KNOW?

Most successful entrepreneurs are not born risk-takers—they develop risk-taking skills through experience.

Characteristics of Successful Entrepreneurs

Successful entrepreneurs are creative and always look for new ideas to solve problems. They are hardworking and remain committed to achieving their goals. Good entrepreneurs are confident and willing to take calculated risks. They have strong decision-making and problem-solving skills. They are also adaptable and can adjust to changing market conditions and customer needs.

Entrepreneurship in Pakistan and the Digital Economy

Entrepreneurship in Pakistan is growing rapidly due to increased access to the internet and mobile technology. Many young people are starting online businesses through social media, e-commerce platforms, and freelancing websites. The digital economy is creating new job opportunities in areas such as software development, digital marketing, and online services. Government and private initiatives are also supporting startups and innovation. This growth is helping improve the country's economy and encouraging youth to become job creators instead of job seekers.

Identifying Business Opportunities

Identifying business opportunities means finding problems in society that can be solved through products or services. Entrepreneurs observe daily life to understand customer needs and market demands. Technology helps in discovering new opportunities such as online education, e-commerce, and digital services. Successful entrepreneurs focus on solving real-world problems in innovative ways. In Pakistan, areas like agriculture, healthcare, and education provide many opportunities for digital business ideas.

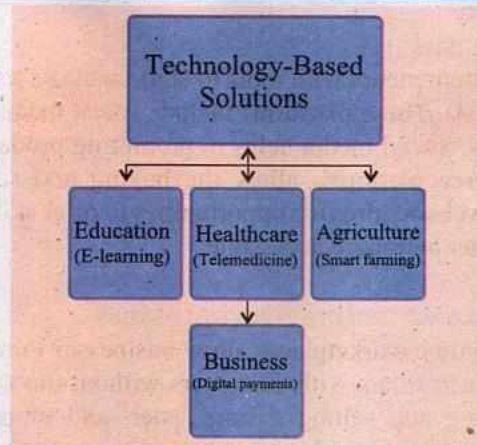


Figure 9.4: Technology-Based Solutions

Solving Real-World Problems Through Technology

Technology helps entrepreneurs solve real-world problems in faster and more efficient ways. It allows people to create digital solutions for challenges in education, healthcare, agriculture, and business (as shown in Figure 9.4). For example, online learning platforms help students study from home, while mobile apps support farmers in improving crop production. Digital payment systems make financial transactions easier and safer. By using technology creatively, entrepreneurs can develop innovative solutions that improve people's daily lives.

Recognizing Market Needs and Customer Demands

Recognizing market needs and customer demands means understanding what people want and what problems they face. Entrepreneurs study customer behavior, preferences, and trends to design better products and services. Surveys, feedback, and online data help identify gaps in the market. Meeting customer needs effectively leads to customer satisfaction and business success. In the digital economy, analyzing online trends and user feedback is very important for creating successful business ideas.

Digital Platforms for Entrepreneurship

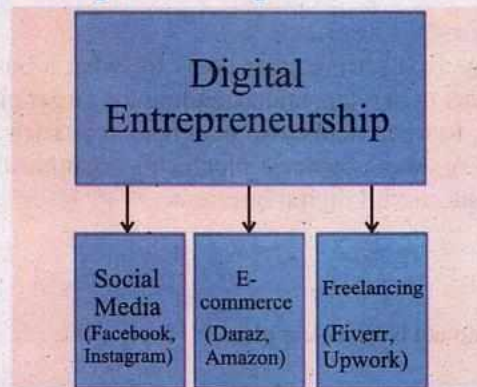


Figure 9.5: Digital Platforms



Using Social Media for Business Promotion

Digital platforms provide entrepreneurs with tools to start, manage, and grow their businesses online (as shown in Figure 9.4). These platforms include social media, e-commerce websites, and freelancing marketplaces. Social media helps in promoting products and reaching a large audience quickly. E-commerce platforms allow the buying and selling of goods without physical shops. Freelancing websites provide opportunities to offer skills and services globally, making entrepreneurship easier and more accessible.

E-commerce Platforms and Online Marketplaces

E-commerce platforms and online marketplaces allow businesses to sell products and services over the internet. They connect sellers with customers without the need for a physical store. These platforms make buying and selling easier, faster, and more accessible to a wider audience. Examples include websites and apps where users can browse products, compare prices, and place orders online. They play an important role in supporting digital entrepreneurship by reducing costs and expanding market reach.

Freelancing and Remote Work Opportunities

Freelancing and remote work allow individuals to offer their skills and services to clients through online platforms. Freelancers can work in areas such as graphic design, writing, programming, and digital marketing. Remote work enables people to work for companies from home or any location with an internet connection. These opportunities help students and professionals earn income independently. They are an important part of digital entrepreneurship as they provide flexibility and global access to job markets.

Planning a Small Digital Business

Planning a small digital business involves organizing ideas into a clear and workable plan. Entrepreneurs first identify a product or service that meets customer needs. They then decide on the target audience, pricing, and method of delivery using digital platforms. A basic budget is prepared to manage costs and expected income. Proper planning helps ensure the business is practical, organized, and more likely to succeed in the digital market.

Basic Business Planning Concepts

Basic business planning involves setting clear goals for what a business wants to achieve. It includes identifying a product or service, understanding the target market, and deciding how to deliver value to customers. Entrepreneurs also plan resources such as time, money, and skills needed to run the business. A simple business plan helps organize ideas and provides direction for starting and growing a successful digital business.

DO YOU KNOW?

Most failed startups do not have a clear plan.



Budgeting and Resource Management

Budgeting and resource management involve planning how money, time, and other resources will be used in a business. A budget helps entrepreneurs estimate costs, set prices, and manage income and expenses effectively. Proper resource management ensures that materials, skills, and tools are used efficiently without waste. In digital businesses, good budgeting and resource planning help maintain profitability and support long-term success.

Teamwork and Communication in Startups

Teamwork and communication are essential for the success of startups and small digital businesses. Team members work together by sharing ideas, responsibilities, and skills to achieve common goals. Effective communication helps avoid misunderstandings and improves decision-making. In startups, clear coordination through meetings, messaging apps, and online tools ensures smooth workflow. Strong teamwork and communication increase productivity and help the business grow successfully.

Innovation and Future Opportunities

Innovation means creating new and improved ideas, products, or services that solve problems in better ways. In digital entrepreneurship, innovation helps businesses grow and stay competitive in the market. Future opportunities are expanding rapidly due to technologies such as artificial intelligence, mobile apps, and online platforms. These technologies are creating new career paths and business ideas for young entrepreneurs. By adopting innovation, individuals can build successful and future-ready digital businesses.

Emerging Technologies and Entrepreneurship

Emerging technologies such as artificial intelligence, cloud computing, blockchain, and mobile applications are transforming entrepreneurship. These technologies help entrepreneurs create smarter, faster, and more efficient business solutions. They reduce costs, improve productivity, and enable global reach through digital platforms. Startups use these technologies to develop innovative products and services that meet modern customer needs. As a result, emerging technologies are opening new opportunities for digital entrepreneurship worldwide.

Role of AI, Apps, and Digital Services in Business

Artificial Intelligence (AI), mobile apps, and digital services play an important role in modern business growth. AI helps entrepreneurs analyze data, understand customer behavior, and improve decision-making. Mobile apps make it easier for businesses to reach customers, sell products, and provide services quickly. Digital services such as online payments, cloud storage, and marketing tools improve efficiency and reduce costs. Together, these technologies support innovation and make businesses more competitive in the digital economy.



DO YOU KNOW?

AI tools can now design, write, and even help run businesses.



Career Pathways in Technology Entrepreneurship

Technology entrepreneurship offers a variety of career pathways for students in the digital age. Individuals can become startup founders by developing and launching their own digital businesses. Others may work as freelancers in fields such as programming, graphic design, and digital marketing. Careers in app development, e-commerce management, and online consultancy are also growing rapidly. With the rise of technology, students can also become innovators who create new digital solutions for real-world problems.

9.5 Ethical, Legal, and Environmental Impacts of Computing

Computing affects many aspects of daily life. Technology can have ethical or unethical effects, legal or illegal consequences, and can impact the environment. Ethical use involves making fair and responsible choices when using digital tools. Legal use follows the laws related to technology. Environmental impact includes energy consumption, electronic waste, and other effects on nature. Awareness of these impacts helps make informed and responsible decisions when using computing resources.

Ethical Use of Technology

Ethical use of technology involves acting responsibly and avoiding harm through digital actions. This includes respecting privacy, fairness, and proper handling of information. Following ethical guidelines helps maintain trust and safety online. Decisions in technology should consider the potential effects on people, organizations, and society. Responsible use of digital tools supports a safe and fair digital environment.



DO YOU KNOW?

Copying online content without permission can violate both copyright laws and digital ethics

Respecting Intellectual Property and Data Ownership

Intellectual property refers to creative work such as software, music, or writing. Data ownership refers to the right to control personal information. Respecting these rights means avoiding copying, sharing, or using work without permission. Personal and sensitive information should be protected and not misused. Legal and ethical respect for intellectual property and data encourages fairness and protects creators and users.

Understanding Consequences of Unethical Digital Behavior

Unethical digital behavior can include hacking, spreading false information, or cyberbullying. Such actions can cause harm, damage reputations, and lead to legal consequences. Even small actions online may have significant effects. Understanding the outcomes of unethical behavior encourages responsible digital conduct. Maintaining ethical standards ensures a safer and more trustworthy online environment.

Legal Aspects and Data Privacy Laws

Legal aspects of computing refer to the rules and regulations that govern the use of technology and digital information. Cybercrime refers to illegal activities carried out using computers, networks, or the internet, such as hacking, identity theft, and online fraud. These laws protect individuals, organizations, and society from misuse of data and technology. Data privacy laws



ensure that personal and sensitive information is collected, stored, and shared responsibly. Understanding these laws helps prevent legal issues and promotes safe digital practices. Compliance with legal frameworks also encourages trust in online systems and services.

Overview of International Frameworks (e.g., GDPR)

The General Data Protection Regulation (GDPR) is a law in the European Union that protects personal data. It sets rules on how organizations collect, store, and use data. GDPR requires transparency, consent, and the right to access or delete personal information. Many countries and companies follow similar standards to ensure data privacy globally. These frameworks aim to prevent misuse of personal information and promote accountability.

Cybercrime Laws and Data Protection Policies in Pakistan

Pakistan has laws to prevent cybercrime and protect digital information. The Prevention of Electronic Crimes Act (PECA) 2016 is the main law in Pakistan that deals with cybercrime. It aims to protect individuals, organizations, and the state from illegal activities carried out using computers, mobile devices, and the internet. These laws cover hacking, identity theft, online fraud, and unauthorized access to data. Organizations are required to follow data protection policies to secure sensitive information. Legal penalties exist for violating cybercrime and data privacy laws. Following these regulations helps maintain security and trust in digital systems within the country.



CLASS ACTIVITY

Students list cybercrimes covered by PECA through a guided worksheet.

Environmental and Social Impacts

Computing affects the environment and society in many ways. Technology can consume energy, produce electronic waste, and contribute to pollution. At the same time, technology influences social behavior, communication, and culture. Understanding environmental and social impacts helps promote responsible use of digital tools. Sustainable practices and awareness of societal effects are important for balancing technology with nature and communities.

E-waste Management and Sustainable Computing

Electronic waste (e-waste) is created when devices are discarded or replaced. Improper disposal of e-waste can harm the environment and human health. Sustainable computing includes recycling, reusing, and reducing electronic devices responsibly. Energy-efficient devices and environmentally friendly practices reduce the negative impact of technology. Proper e-waste management ensures resources are preserved and pollution is minimized.



TIDBIT

Recycling, reusing, and energy-efficient devices reduce environmental harm.

The Role of Technology in Cultural and Societal Change

Technology changes how people communicate, work, and access information. Social media, digital learning, and online services influence culture and daily life. Technology can improve



education, healthcare, and business efficiency. However, it can also create challenges such as digital divide or loss of privacy. Understanding these social impacts encourages thoughtful and responsible use of technology in communities.

Summary

Cybersecurity

Cybersecurity is the practice of protecting computers, networks, data, and online accounts from unauthorized access, misuse, damage, or cyberattacks.

Online Safety

Online safety means using the Internet carefully and responsibly to protect personal information, devices, and digital identity.

Strong Password

A strong password is a secure password that is difficult to guess. It usually includes a combination of uppercase letters, lowercase letters, numbers, and symbols.

Privacy Settings

Privacy settings are options on digital platforms that allow users to control who can see their personal information, posts, profile, location, and online activity.

Privacy Policy

A privacy policy explains how an application, website, or organisation collects, uses, stores, and shares user data.

Digital Collaboration

Digital collaboration means working together online using tools such as Google Workspace, Microsoft Teams, shared documents, video meetings, and group chats.

Digital Etiquette

Digital etiquette refers to polite, respectful, and responsible behaviour while communicating online.

Cyber Threat

A cyber threat is any possible danger to digital systems, data, or users. Examples include phishing, malware, ransomware, hacking, and identity theft.

Phishing

Phishing is a cyberattack in which fake emails, messages, or websites trick users into sharing passwords, bank details, or personal information.

Malware

Malware is harmful software designed to damage a computer, steal data, or disturb normal system operations.

Ransomware

Ransomware is a type of malware that locks files or systems and demands payment to restore access.

Two-Factor Authentication

Two-Factor Authentication (2FA) is a security method that requires two forms of verification, such as a password and a code sent to a mobile phone.

**Biometric Verification**

Biometric verification uses unique physical features, such as fingerprints, face recognition, or voice recognition, to confirm a user's identity.

Firewall

A firewall is a security tool that monitors and controls incoming and outgoing network traffic according to security rules.

Antivirus Software

Antivirus software is a program used to detect, block, and remove viruses and other harmful software from a computer.

Cryptography

Cryptography is the technique of protecting information by converting it into a secure form so that only authorized users can read it.

Data Protection

Data protection means keeping personal, academic, organizational, or sensitive information safe from loss, misuse, theft, or unauthorized access.

Accessibility

Accessibility means designing digital systems so that people with different abilities, needs, and backgrounds can use them easily.

Intellectual Property

Intellectual property refers to creations of the mind, such as software, books, images, videos, designs, and inventions, that are legally owned by individuals or organisations.

Data Privacy Laws

Data privacy laws are legal rules that protect how personal data is collected, stored, used, and shared.

E-Waste

E-waste means discarded electronic devices, such as old computers, mobile phones, batteries, printers, and chargers.

Sustainable Computing

Sustainable computing means using, designing, and disposing of technology in a way that reduces harm to the environment.

Entrepreneurship

Entrepreneurship is the process of creating innovative business ideas, solving problems, and developing opportunities using technology and digital platforms.

Digital Entrepreneurship

Digital entrepreneurship involves using the Internet, social media, e-commerce, or digital tools to create and manage businesses or services.



EXERCISE

Multiple Choice Questions

- The following helps keep online accounts secure:
(a) Weak passwords (b) Strong passwords
(c) Sharing passwords (d) Simple passwords
- The main danger of downloading unknown software is:
(a) Faster browsing (b) Getting rewards
(c) Malware infection (d) Extra storage
- The tool that adds an extra layer of login security is:
(a) Screensaver (b) Two-Factor Authentication
(c) Wallpaper (d) Search engine
- The cyber threat that tricks users into giving personal information is:
(a) Phishing (b) Antivirus
(c) Encryption (d) Backup
- The purpose of a firewall is to:
(a) Delete files (b) Block harmful network traffic
(c) Play games (d) Slow down the computer
- Encryption is used to:
(a) Delete data (b) Make data readable to everyone
(c) Convert data into a secure form (d) Upload data automatically
- A commonly used platform for online collaboration is:
(a) Paint (b) Google Workspace
(c) Notepad (d) VLC Player
- Digital etiquette means:
(a) Sharing all files freely (b) Using rude language online
(c) Safe and polite online behaviour (d) Ignoring team members
- E-waste means:
(a) Old clothes (b) Electronic garbage
(c) Raw materials (d) Food waste
- The international law that protects user privacy is:
(a) HTML (b) GDPR
(c) CPU (d) LAN

Short Questions

- What is the role of strong passwords in protecting data?
- How can downloading suspicious software affect a computer?
- Why is it important to install software updates and security patches?
- What are common types of cyber threats, such as phishing or ransomware?



5. How does Two-Factor Authentication (2FA) improve online security?
6. Who is responsible for managing privacy and security settings on online platforms?
7. What is intellectual property, and why should it be respected in digital use?
8. How does e-waste impact the environment, and what is sustainable computing?
9. Where do international data protection laws like GDPR apply?
10. What is entrepreneurship?



Long Questions

1. Explain the importance of online safety and describe how strong passwords and safe browsing habits protect personal data.
2. Discuss the role of software updates and security patches in maintaining computer security, and explain the risks associated with outdated software.
3. Describe how privacy and security settings on online platforms can be managed. Explain why reading privacy policies is important for data protection.
4. Explain different types of cyber threats such as viruses, phishing, ransomware, spyware, and DDoS attacks. Discuss how these threats can affect both individuals and organizations.
5. Discuss security tools and techniques like Two-Factor Authentication (2FA), biometric verification, firewalls, intrusion detection systems (IDS), and antivirus software. Explain how each helps in protecting data.
6. Explain the concept of entrepreneurship and describe how digital technologies have created new opportunities for entrepreneurs. Include at least three examples of digital entrepreneurship.
7. Explain the legal aspects of computing by discussing international frameworks like GDPR and cybercrime laws and data protection policies in Pakistan. How do these laws protect digital information?
8. Discuss the environmental and social impacts of computing. Explain how e-waste management and sustainable computing practices can reduce harm to the environment, and describe the role of technology in cultural and societal change.



Answer Key

1. B
2. C
3. B
4. A
5. B
6. C
7. B
8. C
9. B
10. C



Instructions for Preparation of Exam Paper of Computer Science and Entrepreneurship for Class XII

ESSENTIAL INSTRUCTIONS FOR PAPER SETTERS

The paper of Computer Science and Entrepreneurship for class XII will consist of 75 marks. Timing of the paper will be 2:30 hours. The paper will be made as per following details:

Part-I: Objective:	Q-1: 15 Multiple Choice Questions will be selected from the entire contents of textbooks; the distribution will be as under: <table><tr><th>Ch #</th><th>MCQ</th></tr><tr><td>01 -----</td><td>02</td></tr><tr><td>02 -----</td><td>02</td></tr><tr><td>03 -----</td><td>02</td></tr><tr><td>04 -----</td><td>02</td></tr><tr><td>05 -----</td><td>02</td></tr><tr><td>06 -----</td><td>02</td></tr><tr><td>07 -----</td><td>01</td></tr><tr><td>08 -----</td><td>01</td></tr><tr><td>09 -----</td><td>01</td></tr></table>	Ch #	MCQ	01 -----	02	02 -----	02	03 -----	02	04 -----	02	05 -----	02	06 -----	02	07 -----	01	08 -----	01	09 -----	01	$1 \times 15 = 15$
Ch #	MCQ																					
01 -----	02																					
02 -----	02																					
03 -----	02																					
04 -----	02																					
05 -----	02																					
06 -----	02																					
07 -----	01																					
08 -----	01																					
09 -----	01																					
Part-II: Subjective:	This section will contain three questions i.e 2,3,4 and each question contain 9 short questions. The distribution will be as under: Q-2: Attempts (6 out of 9) <table><tr><th>Ch #</th><th>SQ</th></tr><tr><td>01 -----</td><td>03</td></tr><tr><td>02 -----</td><td>04</td></tr><tr><td>06 -----</td><td>02</td></tr></table> Q-3: Attempts (6 out of 9) <table><tr><th>Ch #</th><th>SQ</th></tr><tr><td>03 -----</td><td>02</td></tr><tr><td>04 -----</td><td>04</td></tr><tr><td>05 -----</td><td>03</td></tr></table>	Ch #	SQ	01 -----	03	02 -----	04	06 -----	02	Ch #	SQ	03 -----	02	04 -----	04	05 -----	03	$2 \times 6 = 12$ $2 \times 6 = 12$				
Ch #	SQ																					
01 -----	03																					
02 -----	04																					
06 -----	02																					
Ch #	SQ																					
03 -----	02																					
04 -----	04																					
05 -----	03																					



	Q-4: Attempts (6 out of 9) Ch # SQ 07 05 08 02 09 02	$2 \times 6 = 12$
Part-III: Subjective:	This section will contain five long questions and students have to attempt any 3 questions out of 5 questions. Each question carries 8 marks. The detail is as under: Q-5: Ch # Question 01 01 Q-6: Ch # Question 03 01 Q-7: Ch # Question 06 01 Q-8: Ch # Question 08 01 Q-9: Ch # Question 09 01	$3 \times 8 = 24$



Model Paper Computer Science and Entrepreneurship Intermediate part-II

OBJECTIVE

Question 1: Multiple Choice Questions (MCQ)

Encircle the correct answer. Four possible answers A,B,C,D are given to each question. The choice which you think is correct, fill that circle in front of that question with marker or pen ink in the answer book. Cuttings are filling two or more circles will result in zero mark in that question.

Total Marks: 15

Time Allowed: 20 mins

1. Which protocol is mainly used to view web pages?
a. FTP b. DNS c. TCP d. HTTP
2. Which device converts digital signals for internet transmission?
a. Switch b. Hub c. Modem d. NIC
3. Which of the following is a compound proposition?
a. P b. Q c. P AND Q d. True
4. A proposition that is true for at least one case is called:
a. Unsatisfiable b. Invalid c. Satisfiable d. Equivalent
5. Which concept hides data inside a class?
a. Inheritance b. Polymorphism c. Encapsulation d. Abstraction
6. Which keyword is used to define a class in Python?
a. def b. class c. function d. object
7. Which of the following is Python's built-in GUI toolkit?
a. wxPython b. Tkinter c. PyQt d. Kivy
8. What widget is used to get user input in Tkinter?
a. Label b. Button c. Entry d. Listbox
9. Which python module is used for unit testing?
a. numpy b. matplotlib c. unittest d. os
10. Which Python keyword is used for exception handling?
a. try-except b. try-finally c. try-catch d. handle-throw
11. Which metric measures overall correctness of a model?
a. Precision b. Recall c. Accuracy d. F1-score
12. Machine learning allows systems to:
a. Work without data b. Learn from data and improve performance
c. Only store data d. Replace databases
13. Which of the following is a test statistic?
a. Mean b. t-value c. Mode d. Median
14. Which of the following is an example of Cloud Computing?
a. AWS b. MS-Word c. Smartwatch d. USB flash drive
15. What is the main danger of downloading unknown software?
a. Faster browsing b. Malware infection
c. Getting rewards d. Extra storage



Model Paper Computer Science and Entrepreneurship Intermediate part-II

SUBJECTIVE

Total Marks: 60

Time Allowed: 2:10 hours

SECTION I

Q # 2: Write short answers of any six questions from the following: (6*2=12)

- What is network architecture?
- A network architecture experiences a single cable break, and the entire network goes down. Which topology is being used, and why did this failure happen?
- How does **DNS** (Domain Name System) function like a phonebook for the internet?
- Why is propositional logic insufficient for a statement like "All students love coding," making predicate logic necessary instead?
- What it means when a compound statement is called a tautology?
- Formulate a predicate logic statement using variables, a predicate, and a quantifier to represent the sentence: "Someone in this classroom owns a laptop."
- Break down the task of "cleaning a messy bedroom" into three smaller, manageable sub-tasks (Decomposition).
- What is the primary difference between Supervised Learning and Unsupervised Learning?
- Why do we split our data into a training set and a testing set instead of using all of it for training?

Q # 3: Write short answers of any six questions from the following: (6*2=12)

- How does encapsulation help in keeping data secure and private?
- If you have a class called **Player** for a video game, write a single line of code to add an attribute for the player's health and set it to 100.
- You want to clear a text box after a user clicks "Submit". Which **Tkinter** method helps you delete the text inside an **Entry** widget?
- What is the purpose of the **.mainloop()** function in a **Tkinter** program?
- Write a single line of **Tkinter** code to create a window named **root**.
- When a user clicks a "Save" button, your program crashes with an error saying the database table does not exist. Analyze the problem: what step did the programmer forget to do first?
- In debugging, what is a **breakpoint**?
- Explain the difference between a **Syntax Error** (like a typo in code) and an **Exception**.
- Look at this code: **result = 10 / user_input**. If the user types 0, what specific type of built-in Python exception will be raised?

Q # 4: Write short answers of any six questions from the following: (6*2=12)

- What is the main difference between the Null Hypothesis (H_0) and the Alternative Hypothesis (H_a)?



- ii. Why is it considered an ethical issue to completely delete "outliers" (unusual data points) from your dataset just to make your hypothesis look correct?
- iii. If you reject the Null Hypothesis at a 5% significance level ($\alpha = 0.05$), what is the percentage chance that you might be making a mistake and rejecting a true hypothesis?
- iv. Draft a clear Null Hypothesis (H_0) and Alternative Hypothesis (H_a) for an experiment testing whether rolling a standard 6-sided die is fair or biased.
- v. Why is the p-value important in hypothesis testing?
- vi. How Artificial Intelligence is useful in our daily lives? Give two examples.
- vii. How does blockchain ensure security and transparency in transactions?
- viii. How does e-waste impact the environment?
- ix. How can downloading suspicious software affect a computer?

SECTION II

Note: Attempt any three descriptive answers of the following questions: (3*8=24)

- Q. 5: What is OSI model? Explain its layers and their functions? (08)
- Q. 6: Write a Python program to demonstrate multilevel inheritance using Grandfather, Father, and Son. (08)
- Q. 7: Describe model evaluation techniques and explain accuracy, precision, recall and F1-score. (08)
- Q. 8: Discuss the benefits and challenges of Artificial Intelligence (AI) in society. How can ethical principles ensure fair and responsible use of AI? (08)
- Q. 9: Describe how privacy and security settings on online platforms can be managed. Explain why reading privacy policies is important for data protection? (08)



- ii. Why is it considered an ethical issue to completely delete "outliers" (unusual data points) from your dataset just to make your hypothesis look correct?
- iii. If you reject the Null Hypothesis at a 5% significance level ($\alpha = 0.05$), what is the percentage chance that you might be making a mistake and rejecting a true hypothesis?
- iv. Draft a clear Null Hypothesis (H_0) and Alternative Hypothesis (H_a) for an experiment testing whether rolling a standard 6-sided die is fair or biased.
- v. Why is the p-value important in hypothesis testing?
- vi. How Artificial Intelligence is useful in our daily lives? Give two examples.
- vii. How does blockchain ensure security and transparency in transactions?
- viii. How does e-waste impact the environment?
- ix. How can downloading suspicious software affect a computer?

SECTION II

Note: Attempt any three descriptive answers of the following questions: (3*8=24)

- Q. 5: What is OSI model? Explain its layers and their functions? (08)
- Q. 6: Write a Python program to demonstrate multilevel inheritance using Grandfather, Father, and Son. (08)
- Q. 7: Describe model evaluation techniques and explain accuracy, precision, recall and F1-score. (08)
- Q. 8: Discuss the benefits and challenges of Artificial Intelligence (AI) in society. How can ethical principles ensure fair and responsible use of AI? (08)
- Q. 9: Describe how privacy and security settings on online platforms can be managed. Explain why reading privacy policies is important for data protection? (08)



قومی ترانہ

پاک سرزمین شاد باد کشورِ حسین شاد باد
تو نشانِ عزمِ عالی شان ارضِ پاکستان
مرکزِ یقین شاد باد
پاک سرزمین کا نظام قوتِ اخوتِ عوام
قوم، ملک، سلطنت پایندہ تابندہ باد
شاد باد منزلِ مراد
پرچمِ ستارہ و ہلال رہبرِ ترقی و کمال
ترجمانِ ماضی، شانِ حال جانِ استقبال
سایہٴ خدائے ذوالجلال



PUNJAB EDUCATION, CURRICULUM, TRAINING
AND ASSESSMENT AUTHORITY