Cyber Law

---

1. Very Short Answer Questions

(i) **Who was the father of computer ethics?**
The father of computer ethics was Walter Maner.

(ii) **Which is the latest ICT policy?**
The latest ICT policy is the National ICT Policy, 2072 B.S.

(iii) **Name any two areas of cyber laws.**
Two areas of cyber laws are:

1. Digital Signature/Electronic Commerce
2. Intellectual Property Rights

(iv) **Write two examples of cyber crimes.**
Two examples of cyber crimes are:

1. Hacking
2. Cyber Bullying

---

2. Short Answer Questions

(i) **"Cyber laws are very important in present context." Justify this statement.**

Cyber laws are extremely important in the present context because our lives are now heavily reliant on the internet and digital technologies.

- **Protecting Data:** They help protect our personal information, financial details, and sensitive government data from theft and misuse by cybercriminals.

- **Ensuring Trust in E-commerce:** They provide a legal framework for online transactions and e-commerce, ensuring contracts are valid and digital signatures are authentic, which builds public trust in online services.
- **Preventing Crime:** They define and punish various cyber crimes like hacking, phishing, and cyber-terrorism, acting as a powerful deterrent.
- **Maintaining National Security:** They help secure a nation's critical digital infrastructure from foreign or domestic cyberattacks.

(ii) **What is cyber ethics?**
Cyber ethics refers to the moral principles and code of conduct that govern the use of computers, the internet, and other digital technologies. It is about right and wrong behavior in the digital world.

- **Respecting Privacy:** It involves not sharing or using others' personal data without their permission.
- **Respecting Property:** It means not pirating software or illegally downloading copyrighted music and movies (intellectual property).
- **Avoiding Harm:** It dictates that users should not use the internet to harm, bully, or harass others.
- **Acceptable Use:** It promotes the ethical use of IT resources, like not wasting company resources or spreading malware.

(iii) **What do you mean by cyber crime?**
Cyber crime is any criminal activity that involves a computer, a networked device, or the internet. The computer can be the tool used to commit the crime, the target of the crime, or both.

- **Tool:** Using a computer to send phishing emails to steal passwords.
- **Target:** Hacking into a bank's server to steal customer data.
- **Examples:** Common examples include identity theft, creating and distributing viruses, spreading false information, and unauthorized access.

(iv) **Mention the objectives of ICT Policy 2072 BS.**

The ICT Policy 2072 B.S. (Nepal) aims to drive national development through the effective use of information and communication technology. Key objectives include:

- **Digital Access:** To make ICT services accessible to all citizens, including those in remote areas, by promoting infrastructure development.

- **Good Governance:** To promote the use of ICT in government services (e-Government) to make them more efficient, transparent, and quick.
- **Economic Development:** To help create an 'information society' by increasing the production, export, and use of IT services to boost the national economy.
- **Human Resource Development:** To develop skilled and competent human resources in the field of IT through education and training.

---

3. Long Answer Questions

(i) **What do you mean by cyber law? Briefly explain its types.**
Cyber law (or Internet Law) is a branch of law that deals with the legal issues related to the use of Information Technology (IT), computers, and the Internet. It is designed to regulate human behavior in the digital world, address digital crimes, and provide a legal framework for electronic transactions.

Key Types of Cyber Law

Cyber laws are broadly categorized based on the issues they address:

1. Intellectual Property (IP) Laws

- **Focus:** Protects the creations of the mind in the digital space.
- **Explanation:** This covers Copyrights (protecting software code, digital music, videos, and text), Patents (protecting new IT inventions), and Trademarks.
- **Importance:** It ensures that original creators are credited and paid for their work, preventing illegal copying (piracy).

2. Data Protection and Privacy Laws

- **Focus:** Regulating the collection, storage, and use of personal data.

- **Explanation:** These laws give individuals control over their personal information like names, addresses, health data and require organizations to implement strong security measures to prevent data breaches.
- **Importance:** They prevent misuse of personal data and uphold an individual's right to privacy in the digital age.

3. E-commerce and Contract Laws

- **Focus:** Legalizing and regulating online business and transactions.
- **Explanation:** These laws establish the validity of electronic contracts, the acceptance of digital signatures, and set rules for online consumer protection.
- **Importance:** They build trust in online shopping and banking, making electronic commerce legally sound.

4. Cyber Crime Laws (Criminal Law)

- **Focus:** Defining and penalizing crimes committed using the internet.
- **Explanation:** This part of cyber law deals with acts like hacking, phishing (stealing passwords), spreading viruses/malware, cyber-stalking, and denial-of-service (DoS) attacks.
- **Importance:** It provides the legal authority to investigate, prosecute, and punish cyber criminals.

(ii) **Explain cyber law in Nepal in terms of ICT Policy 2072 BS.**

Cyber law in Nepal is largely guided and supported by the National ICT Policy 2072 B.S. (2015 AD), which provides a strategic vision for the digital sector. The policy's goals have driven the development and enforcement of key cyber-related laws.

The Electronic Transactions Act (ETA), 2063 B.S. (2006 AD)

The ETA is the primary cyber law in Nepal. While passed before the 2072 Policy, the policy heavily reinforces its objectives.

- **Legal Recognition of Digital Activities:**
- It gives legal validity to electronic records and digital signatures, which is crucial for e-commerce and e-governance.

- This aligns with the Policy's goal of economic development and promoting ICT usage in government.
- Provisions for Cyber Crime:
- The ETA defines and prescribes punishments for various cyber crimes, such as unauthorized access to a computer system (hacking), spreading false information through digital media, and destruction of computer source codes.
- This supports the Policy's aim to create a safe and reliable digital environment for citizens.

ICT Policy 2072 B.S. and its Impact on Law

The policy outlines the need for a comprehensive legal framework, thereby influencing the direction of cyber law.

- **Focus on Data Security and Privacy:**

  The Policy calls for the establishment of a robust mechanism for data security and cyber-security. While the ETA touches on this, the Policy emphasizes the need for a stronger legal focus on protecting personal and national data, anticipating the development of more dedicated data privacy laws.

- **Support for E-Governance:**

  A major goal of the Policy is to use ICT for good governance. This requires cyber laws to ensure the legality and security of government services like online tax filing or registration. The ETA facilitates this by validating electronic documents.

- **Developing a Legal Human Resource:**

  The Policy recognizes the need to develop legal expertise in cyber law. It encourages training for judges, lawyers, and law enforcement officials to better handle complex cybercrime cases, thus ensuring the effective enforcement of cyber laws like the ETA.

In summary, the ICT Policy 2072 B.S. acts as a roadmap that validates and pushes for the strengthening of Nepal's cyber legal structure, primarily built around the Electronic Transactions Act (ETA), to ensure a secure, transparent, and development-oriented digital future.