Concept 1 : Digital Footprint

Digital footprint: It is the data trail we leave while using the internet on various devices.

It includes our online activities, IP address, and location, which can be used for targeted ads or misused. Being aware of this helps us stay cautious about what we browse, upload, or share online.

Types of Digital footprints:

There are two types of digital footprints: **active** (data we intentionally share, like emails and posts) and **passive** (data collected without our awareness, like browsing history and app usage).

Our digital footprints grow with internet use and are stored in browsers and servers, often beyond our control. Even if we try to erase them, they may still remain. Since digital footprints can reveal user details, location, and device information, it is important to be cautious while being online.

Concept 2 : Net and Communication Etiquettes

Digital Society and Netizen

A **digital society** represents the increasing use of digital technologies in all aspects of life.

A **netizen**(**digital citizen**) is anyone using digital technology and the internet.

Being a **responsible netizen** means following ethical, legal, and safe practices online, including proper net, communication, and social media etiquettes.

Etiquettes are defined as the set of socially accepted behaviors and norms that guide individuals in using information technology responsibly and respectfully.

Net Etiquettes

Net etiquettes refer to the proper manners and behaviors we should follow while interacting online, just as we follow etiquettes in social interactions.

Following are Net Etiquettes:

A) Be Ethical:

- **Avoid copyright violations** by not using or sharing copyrighted materials without permission.
- **Share knowledge responsibly**, ensuring information is accurate, clear, and not redundant.

B) Be Respectful:

- **Respect privacy** by not sharing personal documents, images, or information without consent.
- **Respect diversity** in online discussions, acknowledging differences in culture, experience, and knowledge.

C) Be Responsible:

- **Avoid cyberbullying**, as online harassment has real-world consequences, and actions can be traced through digital footprints.
- **Ignore trolls**, as they provoke arguments for amusement, and the best response is to not engage with them.

Communication Etiquettes

Communication etiquettes refer to the guidelines and proper manners that digital citizens should follow while communicating through emails, chat rooms, social networking sites, and other digital platforms to ensure effective and respectful exchange of ideas, data, and knowledge.

(A)**Be Precise:**

- **Respect time** by avoiding unnecessary responses and not expecting instant replies.
- **Respect data limits** by avoiding large attachments and using cloud storage for sharing files.

(B) **Be Polite:**

- Maintain a respectful tone in both real-time (chat, calls) and delayed (emails, forum posts) communication.
- Avoid aggression or abusive language, even when disagreeing with others.

(C) **Be Credible:**

- Communicate thoughtfully, as credibility is built over time through responsible and reliable interactions.
- People judge credibility based on past comments and responses, so it is important to be mindful of what we share.

Social Media Etiquettes

Social media etiquettes refer to the guidelines and proper behaviors that users should follow while creating, sharing, and interacting on social media platform(facebook, Google+, Twitter, Instagram, Pinterest, You Tube channel) s to ensure respectful, responsible, and effective communication in the digital community.

A) Be Secure:

- **Use strong passwords** and change them frequently to protect accounts from breaches.
- **Be cautious when befriending strangers online**, as their intentions may not always be safe.
- **Verify information before believing or sharing**, as fake news and misinformation are common on social media.

B) Be Reliable:

- **Think before uploading content**, as once shared, it remains stored on remote servers even after deletion. Avoid posting sensitive or confidential data.

Concept 3 : Data Protection, Intellectual Property Rights (IPR), Plagiarism, Licensing and Copyright

1. Data Protection

In the digital age, **data protection** focuses on ensuring the privacy of digitally stored information.

Sensitive data includes biometric, health, financial, and personal information, which, if breached, can cause harm or inconvenience. **Encryption, authentication, and secure methods** help protect such data, ensuring access only to authorized users for legitimate purposes. Globally, **data protection laws** guide the processing, storage, and transmission of sensitive information to prevent unauthorized modification or disclosure.

2. Intellectual Property Right (IPR)

Intellectual Property refers to the inventions, literary and artistic expressions, designs and symbols, names and logos.

Intellectual Property Rights (IPR) protect original ideas, inventions, and creative works, allowing creators to earn recognition or financial benefits.

It is legally safeguarded through copyrights, patents, and trademarks.

(A) Copyright:

Copyright grants legal rights to creators for their original works like writing, photograph, audio recordings, video, sculptures, architectural works, computer software, and other creative works like literary and artistic work.

Copyrights are automatically granted to creators and authors, **preventing unauthorized copying, distribution, or commercial use.**

Example: *The Jungle Book* by Rudyard Kipling is copyrighted, meaning parts of it cannot be used without permission.

(B) Patent:

It Protects inventions, granting the inventor exclusive rights to prevent others from using or selling the invention.

Requires filing an application and is valid for 20 years, after which it can be freely used.

Encourages innovation by allowing inventors to share discoveries while securing financial benefits.

(C) Trademark:

Trademark protects brand identity using unique visual symbol, word, name, design, slogan, label, etc., that distinguishes the brand or commercial enterprise, from other brands or commercial enterprises.

Prevents unauthorized use of similar marks (including words or phrases) that can cause confusion.

Example: Only Nike can use its brand for shoes; a similar name like "Nikke" for shoes would be trademark infringement. However, it may be possible to apply for the Nike trademark for unrelated goods like notebooks.

Licensing

License: A **license** is a type of contract or a permission agreement between the creator of an original work permitting someone to use their work, generally for some price;

Copyright : C**opyright** is the legal right of a creator to protect their original work.

Licensing : The rules about how people can use copyrighted material.

Software License: A **software license** is an agreement that provides legally binding guidelines pertaining to the authorised use of digital material.

Digital content like software, art, literature, photos, etc., is protected as intellectual property. It must be used or shared according to the license rules. Not following these rules is called infringement of Intellectual Property Rights (IPR) and is a criminal offence.

Violation of IPR:

Violation of intellectual property right may happen in one of the following ways:

(A) Plagiarism:

Plagiarism: Copying someone else's work or ideas and presenting them as your own without giving credit to the original creator. It's an ethical offense and can be considered fraud.

(B) Copyright Infringement:

Copyright Infringement: Using someone else's work (like images or text) without their permission or not paying for it when required, even if you mention the source. Just because something is online doesn't mean it's free to use.

(C) Trademark Infringement:

Trademark Infringement: Using someone else's trademark (logo or brand) without permission on products or services. The trademark owner can take legal action against you for this.

Concept 4 : Free and Open Source Software (FOSS)

Freeware	Free Software (open-source software)
Cost-free software (No cost)	Copyright-free software
Software under copyright but available at no cost	Software with no limitations or constraints.

Public Access and Open Source Software

Copyright can limit how others use a work, but public licenses allow people to use, share, and modify the work, encouraging innovation.

Open-source licenses, like **GNU General Public License (GPL)** and **Creative Commons (CC)**, are popular for sharing works freely.

CC is used for all kind of creative works like websites, music, film, literature, etc., while **GPL** applies to software, allowing users to run, modify, and share it.

Unlike freeware, GPL software can be freely distributed and modified.

Proprietary software, is sold commercially and doesn't share its code.

Free and open source software (FOSS) : **Free and Open Source Software (FOSS)** is software that's free to use, with open access to its source code, allowing anyone to modify and improve it.

FOSS Operating Systems: Linux kernel-based operating systems like Ubuntu and Fedora

FOSS tools : office packages like Libre Office, browser like Mozilla Firefox, etc.

Software piracy is the unauthorized use or distribution of software, including making copies without permission, which is a copyright violation.

Using pirated software can harm computer performance, the software industry, and the economy.

****

Creative Commons :

Creative Commons (CC) is a non-profit organization (https://creativecommons.org/) that offers free licenses to help creators share their works globally while giving proper credit. It allows others to use, modify, and share these works without infringing on copyrights.

CC licenses are simple and standardized, enabling free distribution of creative and academic works like art, music, literature, dramatics, movies, images, educational resources, photographs and software.

The CC platform also provides a search tool to find licensed material. Creators can set conditions for how their works are used, resulting in six different types of CC licenses.

Creative Commons (CC) licenses:

1. **CC BY**: Others can use, modify, and distribute your work, even for **commercial purposes**, as long as they credit you.
2. **CC BY-SA**: Others can use, modify, and distribute your work **commercially or non-commercially**, but they must credit you and share their new work under the same license.
3. **CC BY-ND**: Others can reuse your work for any purpose, including **commercially**, but they cannot modify it, and they must credit you.

4. **CC BY-NC**: Others can modify and build upon your work **non-commercially**, and their new work must also be non-commercial and credit you.
5. **CC BY-NC-SA**: Others can remix and build upon your work **non-commercially**, credit you, and license their new work under the same terms.
6. **CC BY-NC-ND**: The most restrictive license, allowing others to download and share your work only if they credit you. They cannot change it or use it commercially.

Concept 5:Cyber crime and cyber laws, hacking, phishing, cyber bullying, overview of Indian IT Act.

Cyber Crime

Cyber crime refers to criminal activities carried out in a digital environment, where computers are either the target or a tool for committing the crime.

These crimes can cause physical harm, financial loss, or mental harassment. Cyber criminals attack computers or networks to damage data, spread viruses or malware, and steal confidential information for blackmail or extortion.

Common cyber crimes include hacking, ransomware attacks, denial-of-service, phishing, email fraud, banking fraud, and identity theft. The frequency of such crimes is increasing rapidly.

A **computer virus** is a type of harmful code that can copy itself and damage or corrupt a computer's data or system.

Malware is software designed to gain unauthorized access to computer systems.

Hacking:

Hacking is unauthorized access to computers, networks or any digital system.

Hackers usually have technical expertise of the hardware and software. They look for bugs to exploit and break into the system.

Ethical hacking (performed by white hat hackers) is done with good intentions, such as testing and improving software security by finding vulnerabilities or loopholes. Ethical hacking is actually preparing the owner against any cyber attack.

Non-ethical hackers, or **black hat hackers (crackers)**, gain unauthorized access to computers or networks to steal sensitive data, damage systems, or cause harm. They use their skills for illegal purposes like identity theft, financial gain, or leaking sensitive information.

Phishing and Fraud Emails:

Phishing is an unlawful activity where fake websites or emails that look original or authentic are presented to the user to fraudulently collect sensitive and personal details, particularly usernames, passwords, banking and credit card details.

Common methods include **email spoofing**, where a fake email address looks similar to a legitimate one, and phishing attempts via phone calls or text messages. These fake communications often use logos and design elements to appear authentic.

(A) Identity Theft : If the **stolen personal data** from computers or computer networks **like** demographic details, email ID, banking credentials, passport, PAN, Aadhaar number, etc., **is used by hackers** to commit fraud on behalf of the victim, it is called identify theft.

This is one type of phishing attack where the intention is largely for monetary gain. There can be many ways in which the criminal takes advantage of an individual's stolen identity.

Criminals may misuse stolen identities in different ways, including **financial identity theft** (for monetary gain), **criminal identity theft** (to hide their true identity), and **medical identity theft** (to obtain medical services or drugs).

Ransomware:

Ransomware is a type of cybercrime where an attacker blocks a user from accessing their computer by encrypting data, then demands payment to restore access.

It can be downloaded from malicious websites, doubtful software repositories, spam emails, or by clicking on harmful ads. The attacker may also threaten to publish sensitive information unless a ransom is paid.

Combatting and Preventing Cyber Crime :

It's important to **stay alert** and **seek legal help**.

Safety measures to reduce the risk of cyber crime:

- Regularly backing up of important data
- Using updated antivirus software
- Avoiding pirated software
- Only downloading from secure websites (https).
- Keep system and application software updated including browser
- Avoid untrusted sites
- Use strong, unique passwords.
- Don't allow browsers to save passwords on shared computers, and use private browsing when necessary. Perform transactions only on trusted sites, and secure home wireless networks with strong, regularly changed passwords.
- For an unknown site, do not agree to use cookies when asked for through a Yes/No option.
- Perform online transaction like shopping, ticketing, and other such services only through well-known and secure sites.

Indian Information Technology Act (IT Act): The growth of the internet has led to an increase in cybercrimes, frauds, and cyberbullying. To address these issues, many countries, including India, have implemented legal measures for protection of sensitive personal data and to safeguard the rights of Internet users.

The Government of India's, Information Technology Act, 2000 (IT Act), amended in 2008, provides guidelines to the user on the processing, storage, and transmission of sensitive information.

It establishes a **legal framework** for electronic governance, recognizing electronic records and digital signatures. The act also defines cybercrimes and their penalties. Additionally, cyber cells in police stations across many Indian states allow individuals to report cybercrimes.

The Cyber Appellate Tribunal was established to resolve disputes related to cybercrimes, such as tampering with computer documents, hacking, using someone else's password, and publishing personal data without consent.

The IT Act enables secure online transactions, allowing people to use credit cards without fear of misuse. It also empowers government departments to file, create, and store official documents in digital format.

Concept 6 : E-Waste : hazards and management

E-waste: Hazards and Management

E-waste(Electronic waste) refers to discarded electronic devices like computers, laptops, mobile phones, televisions, tablets,music systems, speakers, printers, scanners, etc., when they are no longer in use.

It is a growing environmental issue due to the increasing use of electronic products and a lack of awareness on proper disposal methods. **Waste Electrical and Electronic Equipment (WEEE)** is a major concern worldwide, as e-waste makes up more than 5% of municipal solid waste. Proper disposal of e-waste is crucial to minimize harm to the environment and society.

Impact of e-waste on environment:

E-waste contributes to environmental pollution through harmful emissions, liquid waste, and solid materials.

When improperly disposed of in landfills, toxic metals and chemicals from e-waste leach into the soil, causing **soil pollution**. These chemicals can also contaminate groundwater, leading to **water pollution**. Additionally, dust particles with heavy metals pollute the air, contributing to **air pollution**.

Impact of e-waste on humans:

E-waste contains toxic materials like lead, beryllium, cadmium, mercury, and plastics that are harmful to humans, animals, and the environment.

Improper disposal can cause the following problems:

Toxic material	How it will be generated	Diseases
Lead	From monitors and batteries	Lead enters the human body through contaminated food, water, air or soil. Lead poisoning **affects the kidneys, brain and central nervous system.** Children are particularly vulnerable to lead poisoning.
Beryllium	When e-waste such as electronic circuit boards are burnt for disposal	**Skin diseases, allergies and an increased risk of lung cancer**

Copper	Burning of **insulated wires**	**Neurological disorders.**
Mercury	From electronic devices	**Respiratory disorders and brain damage.**
Cadmium	Semiconductors & resistors	**Damage kidneys, liver and bones**
Plastics	From all electronic devices	When this **plastic** reacts with air and moisture, it passes harmful chemicals into the soil and water resources. When consumed, it **damages the immune system of the body and also causes various psychological problems like stress and anxiety.**

Management of e-waste:

E-waste management is the process of properly disposing of electronic waste to minimize harm to humans and the environment, even though it can't be completely destroyed.

Some of the feasible methods of e-waste management are reduce, reuse and recycle.

RRR Reduce, Reuse, Recycle

(1) Reduce: Buy electronic devices based on need, use them fully, and maintain them well to extend their life.

(2) Reuse: **Re-using the electronic or electric waste after slight modification.** Donate or sell functioning devices, and refurbish old electronics for resale.

(3) Recycle: **Recycling is the process of conversion of electronic devices into something that can be used again and again in some or the other manner.** Only those products should be recycled that cannot be repaired, refurbished or re-used. Many companies and NGOs offer door-to-door collection services for recycling.

E-waste Management in India:

In India, the **Environmental Protection Act, 1986** holds individuals or companies responsible for pollution and requires them to pay for the environmental damage caused. The **"Polluter pays Principle"** ensures that violators are punished.

The **Central Pollution Control Board (CPCB)** has set guidelines for the safe disposal of e-waste, making the manufacturers personally responsible for the final disposal of their products when they become e-waste.

The Department of Information Technology (**DIT**), **Ministry of Communication and Information Technology**, has also issued a comprehensive technical guide on "**Environmental Management for Information Technology Industry in India**." The industries have to follow these guidelines for recycling and reuse of e-waste.

In order to make the consumers aware of the recycling of e-waste, prominent smartphone and computer manufacturing companies have started various recycling programs.

Concept 7 : Awareness about health concerns related to the usage of technology

Impact on Health

Spending excessive time in front of screens, such as mobiles, laptops, or televisions, can negatively impact both physical and mental health, especially if done in improper posture.

Overuse of the internet can also lead to addiction and harm well-being. However, these issues can be managed by maintaining good posture and properly positioning devices.

Ergonomics is the science of designing workspaces and equipment for safety and comfort. It helps reduce strain, fatigue, and injuries from prolonged use of devices.

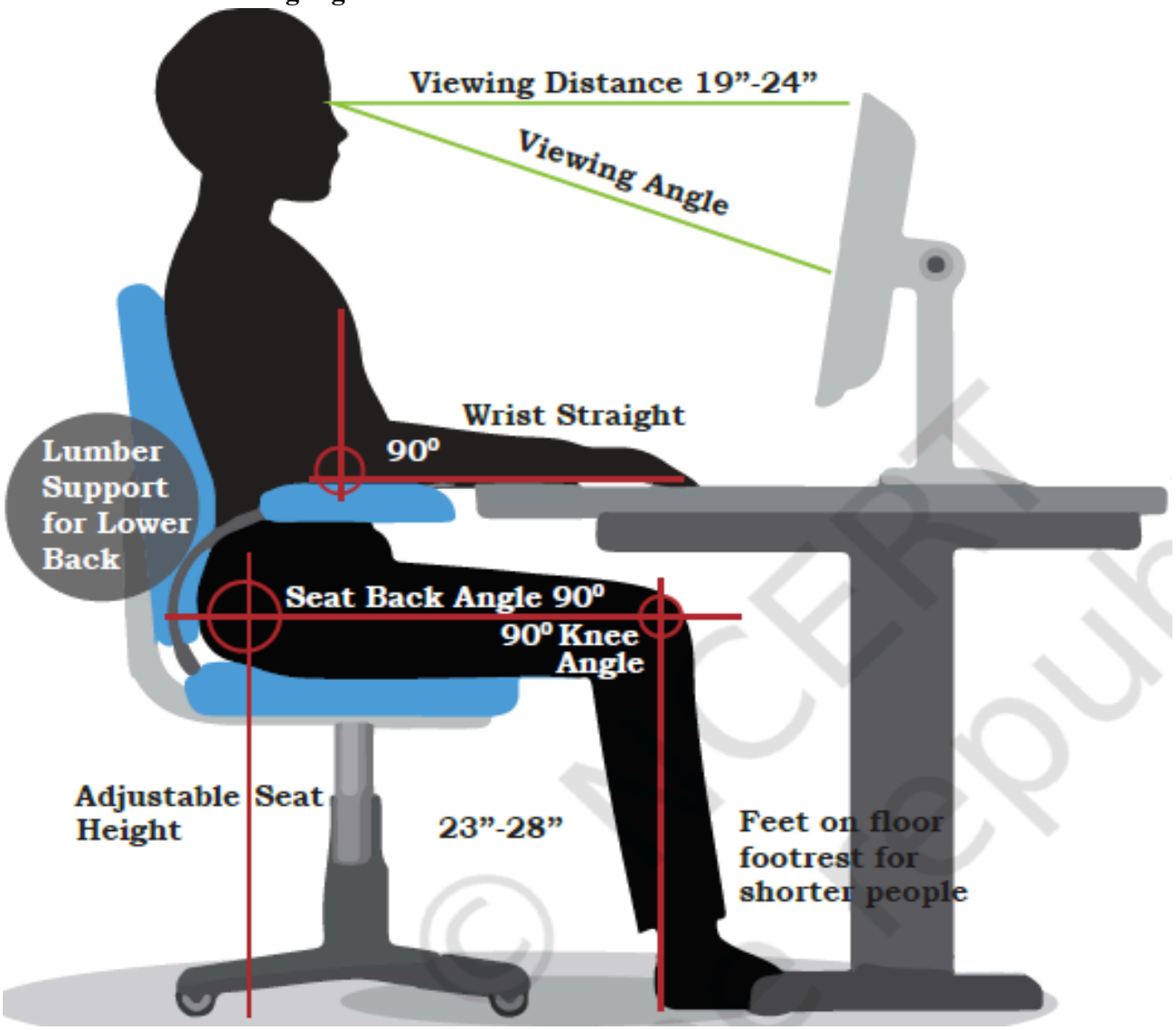
Prolonged screen time, especially on small devices, can cause **eye strain**. Proper posture, viewing distance, and angles can help prevent this.

To avoid eye discomfort like dryness or irritation, it's important to take breaks, focus on distant objects, and engage in outdoor activities.

Bad posture, backaches, neck and shoulder pains can be prevented by arranging the workspace as recommended by ergonomics.

Overuse of keyboards (be it physical keyboard or touchscreen-based virtual keyboard) not aligned ergonomically, can give rise to a **painful condition of wrists and fingers**, and may require medical help in the long run.

Stress, physical fatigue and obesity are the other related impacts the body may face if one spends too much time using digital devices.



Correct posture while sitting in front of a computer

(Information from the image:

- **Viewing Distance**: The distance between your eyes and the screen should be between 19-24 inches.
- **Viewing Angle**: The screen should be positioned at an optimal angle to avoid neck strain.
- **Wrist Position**: Keep your wrists straight to avoid strain.
- **Seat Position**:
  The seat back angle should be 90°.
  The knee angle should also be 90° for proper seating posture.
- **Adjustable Seat Height**: The seat should be adjustable, with the ideal height being between 23-28 inches.
- **Feet Position**: Ensure your feet are flat on the floor, with a footrest for shorter people.
- **Lumber Support**: Use lower back support to avoid strain on the lower back.)