4.1 **Intellectual Property Rights**: Intellectual property rights (IPR) is the term applied to the legal protection afforded to innovative and creative materials. It allows owner of IPR to gain from the use of the material and thereby to encourage innovation and creativity.

**IPR (Intellectual Property Rights) Issues:**

- Copyright law
- The law of confidence
- Patent law
- Design law
- Trademarks
- Copyright and computer programs
- Database copyright and the database right
- Criminal offences

4.2 **Plagiarism**: "The unauthorized use of someone’s ideas, thoughts, expressions and the representation of them as one's own original work."

4.3 **Digital Rights Management**: Digital rights management (DRM) is a systematic approach to copyright protection for digital or electronic media. The purpose of DRM is to prevent unauthorized redistribution of digital media and restrict the ways consumers can copy content they've purchased.

4.4 **Digital License**: A license is an agreement that allows someone to copy, use, or resell the digital content. In digital rights management (DRM), acquiring a license to use protected copyrighted electronic material is essential.

- **Creative Commons license**: A Creative Commons (CC) license is one of several public copyright licenses that enable the free distribution of an otherwise copyrighted "work". A CC license is used when an author wants to give other people the right to share, use, and build upon a work that they (the author) have created.

- **GPL**: The GNU General Public License (GNU GPL or GPL) is a widely-used free software license, which guarantees end users the freedom to run, study, share and modify the software.
• **Apache License:** The Apache License is an open source software license released by the Apache Software Foundation (ASF). ... The Apache License allows you to freely use, modify, and distribute any Apache licensed product. However, while doing so, you're required to follow the terms of the Apache License.

### 4.5 Open Source Software:
- Freely used and freely accessible
- Source code is open and freely available
- Less permissive than free software
- No payment required
- Example:
  - **Linux:** Free software and Open source Development
  - **Apache Server:** Open source web server
  - **MySql:** Open source database system
  - **Pango:** Open source framework
  - **Tomcat:** Open source servlet container
  - **PHP:** Open Source Programming Language
  - **OpenOffice:** Open office application suite
  - **Python:** interpreted, interactive programming language

### 4.6 Open Data:
Open data is data that anyone can access, use and share without any copyright restrictions. Governments, businesses and individuals can use open data to bring about social, economic and environmental benefits. Open data must also be licensed to allow free usage and be available for commercial use. It has the power to help improve services, grow economies and protect our planet.

*Example:*
- Government policies and implementation
- Money spent on government projects
- Surveys

### 4.7 Privacy Laws:
Privacy law refers to the laws that deal with the regulating, storing, and using of personal information of individuals, which can be collected by governments, public or private organizations, or other individuals.

**Types of privacy laws:**

(i) **General Privacy law:** related to personal information of an individual.
(ii) **Specific Privacy law:** designed to regulate specific types of information. Example: Financial, Health, communication, information privacy law.
In India, there is a fundamental right to privacy under the Indian constitution, establishing that “The right to privacy is protected as an intrinsic part of the right to life and personal liberty”.

“Every individual in society irrespective of social class or economic status is entitled to the intimacy and autonomy which privacy protects. The pursuit of happiness is founded upon autonomy and dignity. Both are essential attributes of privacy which makes no distinction between the birth marks of individuals.”

The Information Technology (Amendment) Act, 2008 made changes to the Information Technology Act, 2000 and added the following two sections relating to Privacy:

- Section 43A, which deals with implementation of reasonable security practices for sensitive personal data or information and provides for the compensation of the person affected by wrongful loss or wrongful gain.
- Section 72A, which provides for imprisonment for a period up to three years and/or a fine up to Rs. 500,000 for a person who causes wrongful loss or wrongful gain by disclosing personal information of another person while providing services under the terms of lawful contract. A constitutional bench of the Supreme Court declared 'Privacy' as a fundamental right on 24 August 2017

4.8 Fraud:
- Fraud is intentional deception over internet to secure unfair or unlawful gain, or to deprive a victim of a legal right.
- Fraud can violate civil law, a criminal law.
- It refers to dishonestly cheating someone.

4.9 Cyber Crime: Criminal activities carried out by means of computers or the Internet. There are some examples of cybercrime:

(i) **Phishing**: Phishing is the fraudulent act of acquiring private and sensitive information (username and password) of a person or company through e-mail, malicious links etc.

(ii) **Illegal downloads**: Illegal downloading is obtaining files that you do not have the right to use from the Internet. Downloading of copyrighted files for which you do not have permission or licensed, is called illegal downloads.

(iii) **Child Pornography**: Sexual exploitation of children (under the age of 18). Child pornography is publishing and transmitting obscene material of children in electronic form. Child pornography is most often made by taking pictures, audio and video recording.

**Safeguards for children:**
- Never give address to people who you do not know.
- Never publish your personal information publicly.
- Do not open suspicious emails.
- Never visit porn, harmful websites.

Child pornography is a crime in India. Information Technology Act, 2000 & Indian Penal Code, 1860 provides protection from child pornography. Child is the person who is below the age of 18 years.

The newly passed Information Technology Bill is set to make it illegal to not only create and transmit child pornography in any electronic form, but even to browse it.

The punishment for a first offence of publishing, creating, exchanging, downloading or browsing any electronic depiction of children in “obscene or indecent or sexually explicit manner” can attract five years in jail and a fine of Rs. 10 lakh.

(iv) Scams: A scam is a term used to describe any fraudulent business or scheme that takes money or other goods from an unsuspecting person.

Types of scams:

- **Phishing:** fraudulent act of acquiring private and sensitive information
- **Auction Fraud:** someone may claim to be selling tickets for an upcoming concert that really are not official tickets.
- **Donation Scam:** A person claiming they have or have a child or someone they know with an illness and need financial assistance.
- **Catfish:** A person who creates a fake online profile with the intention of deceiving someone.
- **Cold call scam:** Someone claiming to be from technical support from a computer company, saying they have received information that your computer is infected with a virus, or hacked. They offer to remotely connect to your computer and fix the problem.
- **Chain main:** Usually harmless, this scam is usually spread through e-mail and tells people to forward the e-mail to all their friends to get money back from someone.
- **Online survey scams:** Online survey scams are survey sites that say they offer money or gift vouchers to participants.

4.10 Cyber Forensics: Cyber forensics is a technique of digital forensic science for investigation and analysis to collect evidence from a computer, mobile, internet or any electronic device to present evidence in court of law, against any criminal activity.

4.11 Information Technology Act, 2000

The Information Technology Act, 2000 (also known as IT Act-2000) is an Act of the Indian Parliament notified on 17 October 2000. It is the primary law in India dealing with cybercrime and electronic commerce.

The original Act contained 94 sections, divided in 19 chapters and 4 schedules. The laws apply to the whole of India. Persons of other nationalities can also be indicted under the law, if the crime involves a computer or network located in India.
The Act provides legal framework for electronic governance by giving recognition to electronic records and digital signatures.

Commission of cybercrime may be divided into three basic groups:

- Individual
- Organisation
- Society at Large

**Against Individual**
- Harassment via Emails
- Cyber Stalking
- Dissemination of obscene material
- Defamation
- Hacking/Cracking Indecent Exposure
- Computer Vandalism
- Transmitting a Virus
- Network Trespassing
- Unauthorized Control over Computer System
- Hacking/Cracking

**Against Organisation**
- Hacking & Cracking
- Possession of unauthorized Information
- Cyber- Terrorism against Government Organization
- Distribution of Pirated Software Etc

**Against Society at Large**
- Pornography
- Polluting the youth through indecent exposure
- Trafficking

**Offenses UNDER THE IT ACT, 2000**

1. **Tampering with computer source documents (Intellectual Property):**

   **Section 65** of this Act provides that Whoever knowingly or intentionally conceals, destroys or alters or intentionally or knowingly causes another to conceal, destroy or alter any computer source code used for a computer, computer program, computer system or computer network, when the computer source code is required to be kept or maintained by law for the being time in force, shall be punishable.

   **Punishment** : This is cognizable and non- bailable offense. Imprisonment up to 3 years and or fine up to two lakh rupees.
2. Hacking with the computer system:

Section 66 provides that-

(1) Whoever with the intent to cause or knowing that he is likely to cause wrongful loss or damage to the public or any person destroys or deletes or alters any information residing in a computer resource or diminishes its value or utility or affects it injuriously by any means, commits hacking.

(2) Whoever commits hacking shall be punished with imprisonment up to three years, or with fine which may extend up to two lakh rupees, or with both.

Punishment: Imprisoned up to three years and fine which may extend up to two lakh rupees or with both.

3. Publishing of obscene information in electronic form:

Section 67 of this Act provides that whoever publishes or transmits or causes to be published in the electronic form, any material which is about posting obscene, defamatory and annoying message about a person.

Punishment: On first conviction with imprisonment of either description for a term which may extend to five years and with fine which may extend to one lakh rupees and in the event of a second or subsequent conviction with imprisonment of either description for a term which may extend to ten years and also with fine which may extend to two lakh rupees.

4. Power of Controller to give directions:

Section 68 of this Act provides that:

(1) The Controller may, by order, direct a Certifying Authority or any employee of such Authority to take such measures or cease carrying on such activities as specified in the order if those are necessary to ensure compliance with the provisions of this Act, rules or any regulations made thereunder.

(2) Any person who fails to comply with any order under sub-section (1) shall be guilty of an offense and shall be liable on conviction to imprisonment for a term not exceeding three years or to a fine not exceeding two lakh rupees or to both.

Punishment: The offense under this section is non-bailable & cognizable. Imprisonment up to a term not exceeding three years or fine not exceeding two lakh rupees.

5. Directions of Controller to a subscriber to extend facilities to decrypt information:

Section 69 provides that-

(1) If the Controller is satisfied that it is necessary or expedient so to do in the interest of the sovereignty or integrity of India, the security of the State, friendly relations with foreign States or public order or for preventing incitement to the commission of any cognizable offense; for reasons to be recorded in writing, by order, direct any agency of the Government to intercept any information transmitted through any computer resource.
(2) The subscriber or any person in charge of the computer resource shall, when called upon by any agency which has been directed under sub-section (1), extend all facilities and technical assistance to decrypt the information.

(3) The subscriber or any person who fails to assist the agency referred to in subsection shall be punished with imprisonment for a term which may extend to seven years. Punishment: Imprisonment for a term which may extend to seven years. The offense is cognizable and non-bailable.

6. Protected System:

Section 70 of this Act provides that —

(1) The appropriate Government may, by notification in the Official Gazette, declare that any computer, computer system or computer network to be a protected system.
(2) The appropriate Government may, by order in writing, authorize the persons who are authorized to access protected systems notified under sub-section (1).
(3) Any person who secures access or attempts to secure access to a protected system in contravention of the provision of this section shall be punished with imprisonment of either description for a term which may extend to ten years and shall also be liable to fine.

Punishment: The imprisonment which may extend to ten years and fine.

7. Penalty for misrepresentation:

Section 71 provides that—

(1) Whoever makes any misrepresentation to, or suppresses any material fact from, the Controller or the Certifying Authority for obtaining any license or Digital Signature Certificate, as the case may be, shall be punished with imprisonment for a term which may extend to two years, or which fine which may extend to one lakh rupees, or with both.

Punishment: Imprisonment which may extend to two years or fine may extend to one lakh rupees or with both.

8. Penalty for breach of confidentiality and privacy:

Section 72 provides that- Save as otherwise provide in this Act or any other law for the time being in force, any person who, in pursuance of any of the powers conferred under this Act, rules or regulation made thereunder, has secured assess to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

Punishment: Term which may extend to two years or fine up to one lakh rupees or with both.

9. Penalty for publishing Digital Signature Certificate false in certain particulars:

Section 73 provides that—

(1) No person shall publish a Digital Signature Certificate or otherwise make it available to any other person with the knowledge that—
(a) The Certifying Authority listed in the certificate has not issued it; or
(b) The subscriber listed in the certificate has not accepted it; or
(c) The certificate has been revoked or suspended unless such publication is for the purpose of verifying a digital signature created prior to such suspension or revocation.
(2) Any person who contravenes the provisions of sub-section (1) shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees, or with both.

**Punishment:** Imprisonment of a term of which may extend to two Years or fine may extend to 1 lakh rupees or with both.

10. **Publication for fraudulent purpose:**

**Section 74** provides that- Whoever knowingly creates, publishes or otherwise makes available a Digital Signature Certificate for any fraudulent or unlawful purpose.

**Punishment:** Imprisonment for a term up to two years or fine up to one lakh or both.

11. **Act to apply for offense or contravention committed outside India:**

**Section 75** provides that-

(1) Subject to the provisions of sub-section (2), the provisions of this Act shall apply also to any offense or contravention committed outside India by any person irrespective of his nationality.

For the purposes of sub-section (1), this Act shall apply to an offense or Contravention committed outside India by any person if the act or conduct constituting the offense or contravention involves a computer, computer system or computer network located in India.

12. **Confiscation:**

**Section 76** provides that- Any computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, in respect of which any provisions of this Act, rules, orders or regulations made thereunder has been or is being contravened, shall be liable to confiscation. :

Provided that where it is established to the satisfaction of the court adjudicating the confiscation that the person in whose possession, power or control of any such computer, computer system, floppies, compact disks, tape drives or any other accessories relating thereto is found is not responsible for the contravention of the provisions of this Act, rules orders or regulations made thereunder, the court may, instead of making an order for confiscation of such computer, computer system, floppies, compact disks, tape drives or any other accessories related thereto, make such other order authorized by this Act against the person contravening of the provisions of this Act, rules, orders or regulations made thereunder as it may think fit.

https://pythonschoolkvs.wordpress.com/
13. Penalties or confiscation not to interfere with other punishments:

Section 77 provides that – No penalty imposed or confiscation made under this Act shall prevent the imposition of any other punishment to which the person affected thereby is liable under any other law for the time being in force.

Power to investigate offenses:

Section 78 provides that – Notwithstanding anything contained in the Code of Criminal Procedure, 1973, a police officer not below the rank of Deputy Superintendent of Police shall investigate any offense under this Act.

4.12 Technology and Society:

Technology impacts the environment, people and the society as a whole. The way we use technology determines if its impacts are positive to the society or negative.

<table>
<thead>
<tr>
<th>Positive Impacts</th>
<th>Negative Impacts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Can send and access information anytime, anywhere.</td>
<td>Threat of online predators like hackers, viruses, fraud, scams etc.</td>
</tr>
<tr>
<td>Long distance communication</td>
<td>Loss of personal contact</td>
</tr>
<tr>
<td>Automation</td>
<td>Overdependence</td>
</tr>
<tr>
<td>Improved transportation</td>
<td>Natural resource Depletion</td>
</tr>
<tr>
<td>Improved Education and learning process</td>
<td>Increased pollution</td>
</tr>
<tr>
<td>Improvement in agriculture</td>
<td>Wastage of time with online games and social media</td>
</tr>
<tr>
<td>Improvement in health facilities</td>
<td>Less physical growth</td>
</tr>
<tr>
<td>Business and banking</td>
<td>Impact of ethics and human values</td>
</tr>
<tr>
<td>Online shopping</td>
<td>Global warming</td>
</tr>
<tr>
<td>Satellite communication</td>
<td>Nuclear bomb and weapons</td>
</tr>
</tbody>
</table>

Cultural Impact of Technology:

1. Tradition: The influence of IT on religious practices has mainly been to the effect of making information about them more accessible.

2. Government: It helps government to improve its services to citizens.

Collection of data of citizens may help government to provide better services according to their need. But it may lead fraud and scam, if data is not preserved securely.

3. Defence: Defence capabilities are improved.

4. Commercial business: Able to extract information what the customer wants. Easy to transport the products.

5. Encourages innovation and creativity

6. Improves on human resource management.

7. Ethics, human values, customs and culture degraded.
4.13 E-waste Management:

E-waste stands for Electronic waste. E-waste is actually the old electronic items that people simply give away to garbage trucks that are then dumped into landfill. Electronics have a number of harmful elements that react with air and water to create problems of e-waste such as water, air and soil pollution as well as problems that affect human beings in the form of diseases. E-waste management is required to overcome this problems.

**Definition**: Proper disposal of electronic equipment and its impact on environment, is known as e-waste management. It includes reuse, resale, recycling of electronic devices.

**E-waste management rules, 2011**:  
Extended Producer Responsibility (EPR) principle will apply Collection of E-waste :

- Generated during manufacturing
- Generated from the end of life products
- Such E Wastes are channelized to a registered dismantler or recycler
- Individual identification code for product tracking
- Provide contact details of dealers and authorized collection centers to consumers
- Finance and organise the system
- Ensure safe transportation, storage
- Submit annual return

**How to manage e-waste:**

- Buy less
- Follow the EPR strategy : The EPR is an environment protection strategy that makes the producer responsible for the entire life cycle of the product, specially for take back, recycle and final disposal of the product
- Organize what you have
- Donate your e-waste
- Use buy-back method
- Learn about your local recycling options
- Live in the cloud
- Follow RRR (Reduce, Reuse, Recycle)
  - **Reduce**: Reduce the use of electronic items.
  - **Reuse**:
    - Plastic
    - Metal
    - Glass
    - Printed Circuit board
    - Hard Drives
- Cartridges
- Batteries

**Recycle:**
- Picking Shed: Sort the items manually. Remove batteries
- Disassemble
- First size reduction process
- Second size reduction process
- Over band magnet
- Separation of metallic and non-metallic components
- Water separation

### 4.14 Identity Theft

**Identity Theft:** when someone uses your personal information to pretend to be you without your knowledge and commit a crime or fraud.

**How to prevent Identity Theft:**

- Never share your password or account number over email or message.
- Do not follow links from e-mails when performing financial transaction.
- Be aware of callers, pop-ups, websites or emails asking for personal information.
- Use firewall and reliable anti-virus software.
- Never share your personal information in public domain.
- Regularly change the passwords of your account.

### 4.15 Unique Ids

**Unique Ids:** Unique ids include fingerprints, hand geometry, earlobe geometry, retina and iris patterns, voice waves, DNA, and signatures.

**Iris Pattern:** Iris recognition is an automated method of biometric identification that uses mathematical pattern-recognition techniques on video images of one or both of the irises of an individual's eyes, whose complex patterns are unique, stable, and can be seen from some distance.

### 4.16 Biometrics

**Biometrics:** Electronic device which is used for authentication and identification of a person using his/her biological and behavioural characteristics.

### 4.17 Gender and disability issues while teaching and using computers:

The low participation by women in computer science courses in secondary and sr. secondary education is an important equity issue in science education. In addition to the increasingly intense need for more highly skilled people in the IT sector, women are missing out on many of today’s most attractive career opportunities. Equally importantly, the IT field is missing out on the broader range of perspectives and talents that would result from significantly increased participation by women.

To overcome this stereotype situation, the following points to be noted:

Transform pink software by creating gender neutral software that challenges and appeals to a variety of students;
- Look to girls and women to fill the IT job shortage: encourage girls into computing by using technology in a broad range of subjects to attract a more diverse group of students.
- Prepare tech-savvy teachers: empowered teachers will empower students.
- Educate girls to be designers, not just users, ensuring they have opportunities to fully explore the potential of technology.
- Change the public face of computing so girls have a realistic image of computer professionals, and understand the importance of communication and team work in this field.
- Create a family computer, placed where the entire family has access, and computer activities are associated within a social context, and not equated to isolation.
- Set a new standard for gender equity that seeks equal contributions to innovations in technology and equal mastery of the analytical and computing skills required to make these contributions.