

## Social & Professional Issues in IT (2-1-0)

### Objective:

This course aims to provide knowledge for handling social, professional and legal issues that arise in the working environment of IT

### Course Outline:

1. History of Computing
2. Social Context of Computing
3. Computer Ethics and Ethical Theories
4. Professional Ethics
5. Risk and Responsibilities
6. Privacy
7. Computer and Cyber Crimes
8. Intellectual Property and Legal Issues

1

### Textbooks:

- Johnson, D. G., Computer Ethics, Pearson Education Asia, Third Edition
- IT Policies and Laws of the government of Nepal

### References:

- Hussain, K. M., and Hussain, D. S., Computers; Technology, Applications, and Social Implications, PHI, New Delhi, ISBN: 81-203-0620-1.
- Sara Baase, Gift of Fire, A: Social, Legal, and Ethical Issues for Computer and Internet
- Articles collected from various Journals and Periodicals, such as IEEE-Computer, BYTE, ACM Periodicals, etc.

2

### Evaluation:

- 50 Internal + 50 Final Exam(by Exam Office) = 100  
(Internal 50 = theory 30 + practical 20)

#### Internal evaluation methods:

- Internal examination(s)
- Attendance
- Assignment(s)/Case studies
- Class Performance

3

## 1. History of Computing

- Start with beginning of the civilization
- Evolved as a result of man's search for fast and accurate calculating devices
- Provide the birth of computer and digital technology further enhancing as an information technology

**Information Technology:** Use of technologies/devices to collect, store, manage, process and dissemination/communication of information. This encompasses a wide range of computer, network and internet based technologies/devices and services.

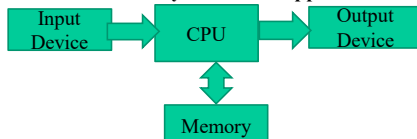
### Computer:

- An electronic programmable device which receives data as an input, process it and provide information as an output
- Contains following components:
  - i. **Hardware component:** Physical components of a computer, which may be electronic, electrical, magnetic, mechanical or optical and are:
    - Input device -Output device -Memory -Central processing unit (CPU)

— ii. **Software Component:** Logical component contain set of *programs* written for a computer to do task and guide computer to perform a work

- It may be (Types of Software):

-System software -Utility software -Application software



Schematic (Block) diagram of a computer

**Network:** A network refers to a group of interconnected elements or components that work together to achieve a common goal

**Networking:** the practice of connecting two or more devices together to facilitate communication between them

**Internet:** Worldwide networks of computers that enables communication and information sharing globally

## 1. 1 Prehistory of Computing

- The prehistory of computing refers to the period of human history before the development of modern computers and digital technology that became backbone for invention of computers
- Today's digital computers are possible due to invention of various computing devices some of them are:
  - The Abacus
  - Pascal & Leibniz's Mechanical Machine
  - Babbage and his Engine
  - ENIAC (Electronic Numerical Integrator and Calculator)
  - Von-Neumann and Stored Programming Concept
  - UNIVAC (Universal Automatic Computer)

6

## 1.2 History of Computer Hardware

The history of computer hardware can be traced back to the early 19th century when Charles Babbage designed the prototype of first mechanical computer, known as the Difference Engine. However significantly started with

- Vacuum tubes used by ENIAC, first general electronic computer
- Transistors
- IC's, LSI and MSI
- LSI and VLSI i.e, Microprocessor
- ULSI, Bio-chips

### 1.3 History of Software: Programming languages and Operating systems

The history of software can be traced with evolution programming languages here's a brief overview of the development of programming languages and operating systems:

7

## 1.3 History of s/w...

### Programming Languages:

- **Machine language (1940s):** The earliest computers were programmed in machine language, which is a binary code understood by the computer's hardware.
- **Assembly language (1950s):** Assembly language was developed as a way to make programming easier and more human-readable. It uses mnemonic codes to represent machine language instructions.
- **FORTRAN (1957):** FORTRAN (Formula Translation) was the first high-level programming language, designed for scientific and engineering applications.
- **COBOL (1959):** COBOL (Common Business Oriented Language) was developed for business applications.
- **BASIC (1964):** BASIC (Beginner's All-purpose Symbolic Instruction Code) was developed for beginners and educational purposes.
- **C (1972):** C was developed as a systems programming language, used for operating systems and low-level programming.
- **Java (1995):** Java was developed as a platform-independent language for web-based applications.
- **Python (1991):** Python is a high-level, interpreted language used for scripting, automation, and data analysis.

## 1.3 History of s/w...

### Operating Systems:

- **Batch processing systems (1950s):** The earliest operating systems were designed for batch processing, where jobs were submitted to the computer in batches and processed sequentially.
- **Time-sharing systems (1960s):** Time-sharing systems allowed multiple users to share a computer simultaneously, with each user having the illusion of having their own computer.
- **Unix (1969):** Unix was developed as a multi-user, multi-tasking operating system, designed to be portable and scalable.
- **MS-DOS (1981):** MS-DOS (Microsoft Disk Operating System) was developed for IBM-compatible PCs, and became the dominant operating system for personal computers in the 1980s.
- **Windows (1985):** Windows was developed as a graphical user interface for MS-DOS, and later became a standalone operating system.
- **Linux (1991):** Linux is a free, open-source operating system based on Unix, and is widely used for servers, supercomputers, and embedded systems.

## 1.4 History of Networking

The history of networking can be traced back to the 1960s, when computer systems began to be used for scientific research and military purposes. At that time, computers were primarily standalone systems that were not connected to each other. **However**, the age of networking began with the inventions of the telegraph, the telephone, the radio, and the television.

- In the late 1960s, the U.S. Department of Defense started developing a networking technology called ARPANET (Advanced Research Projects Agency Network) to enable communication and data exchange between different research institutions. ARPANET was based on packet switching technology, which allowed the transmission of data in small packets over multiple paths.
- In the 1970s, ARPANET grew in popularity and other networking technologies were developed. In 1974, the Transmission Control Protocol (TCP) was developed, which allowed different networks to communicate with each other. This led to the creation of the Internet Protocol (IP), which formed the basis of the modern internet.

## 1.4 History...

- In the 1980s, local area networks (LANs) were developed, allowing computers within a limited geographical area to connect to each other. Ethernet, which was developed by Xerox in the 1970s, became the dominant LAN technology.
- In the 1990s, the World Wide Web was developed, providing a user-friendly interface for accessing information over the internet. The use of the internet exploded in popularity, with the development of web browsers and search engines.
- In the 2000s, wireless networking became popular, with the development of Wi-Fi technology. Mobile devices such as smartphones and tablets also became widespread, leading to the development of mobile networks and mobile internet.
- Today, networking continues to evolve with the development of new technologies such as the Internet of Things (IoT), 5G wireless networks, and software-defined networking (SDN).

## 1.5 Pioneers of Computing

The field of computing has been shaped by the work of numerous pioneers over the years. Here are some of the figures:

- **Ada Lovelace:** Ada Lovelace is considered to be the world's first computer programmer. She worked with Charles Babbage on his Analytical Engine and wrote the first algorithm intended to be carried out by a machine.
- **Alan Turing:** Alan Turing is known as the father of modern computing. He helped crack Nazi codes during World War II and developed the concept of the universal Turing machine, which is considered to be the foundation of modern computing.
- **Grace Hopper:** Grace Hopper is known for developing the first compiler, a program that translates source code into machine code. She also helped develop the programming language COBOL.

12

## 1.5 Pioneers ...

- John von Neumann: John von Neumann made significant contributions to the development of computer architecture and the design of digital computers. He also helped develop the first electronic computer, the ENIAC.
- Steve Jobs and Steve Wozniak: The co-founders of Apple, Steve Jobs and Steve Wozniak, helped revolutionize the personal computer industry with the introduction of the Apple II in 1977.
- Bill Gates: Bill Gates co-founded Microsoft, which has played a significant role in the development of personal computing and software.
- Tim Berners-Lee: Tim Berners-Lee is credited with inventing the World Wide Web, which revolutionized the way people access and share information on the internet.

These are just a few examples of the many pioneers who have contributed to the development of computing. Their work has paved the way for the technology we use today.

13

## 2. Social Context of Computing

- Study of impact that computer technology has on society and the ways in which social factors play the role in the development and use of computing technology
- Includes how people interact with computers, how computers are designed and marketed, and how can be used in different contexts, further deals with **society and technology, internet and society, E-Governance and E-Government Systems** etc.

### 2.1 Society and Technology

- Interconnected and have a significant impact to each other, include study of various aspects of society and technology such as **impact of technology on society and vice versa, using technology for poverty alleviation, health related issues for an IT professional** etc.
- Technology an application of scientific knowledge to create tools, products, and services that improve our life is a product of **society**
- Society a group of individuals who share a common culture, values, institutions and knowledge using **technology** for the betterment of our lives, work, and interact

## 2. Social...

### 2.1.1 Impact of Technology on Society and Vice Versa

- Technology and society have a close relationship, with each influencing and developing the other
- Technology fulfils the needs of society and social values as well as needs direct the evolution of technology

#### Impact of Technology on Society:

- Communication
- Economic growth
- Healthcare
- Environment

#### Impact of Society on Technology:

- Social values
- Legal and ethical considerations
- Consumer demand

15

## 2. Social...

### 2.1.2 Using Technology for Poverty Alleviation

Technology can play a major role in poverty alleviation by improving access to essential services and creating new economic opportunities such as:

- Digital Financial Services
- Agricultural Technology
- Health Technology
- Education Technology etc

### 2.1.3 Health Related Issues for an IT Professional

Working in the field of IT can involve long hours of sitting in front of and using a computer, which can lead to various health-related issues such as:

- Eye Strain
- Repetitive Strain Injury
- Back Pain
- Stress and Mental Health
- Internet Addiction

16

## 2. Social...

### 2.2 Internet and Society

Internet has impact on society in a variety of ways such as:

- Global Connectivity
- Information Access
- Commerce and Business
- Social and Political Impacts

however it has several risks and challenges that need to be addressed such as **digital divide and bridging the digital divide, governance of internet** etc.

#### 2.2.1 Digital Divide and Bridging the Digital Divide

- The situation in which some people have access to modern information technology while others do not
- caused by a variety of factors, including geographic location, socioeconomic status, and educational level

17

### 2.2.1 Digital Divide ...

- Need to be addressed for **bridging it** to ensure that everyone has access to technology for education, employment, and other essential services for advancement of lives with the help of following approaches:

- Infrastructure development
- Digital Literacy Training
- Affordable Technology
- Public-Private Partnerships
- Community Centers

#### 2.2.2 Governance of Internet

Governance of internet is the organizations and processes responsible for managing and regulating the internet. Although it is a complex and evolving issue but here are some key stakeholders and approaches to internet governance:

### 2.2.2 Governance of Internet...

- Multistakeholderism
- Government Regulation
- Technical Standards Organizations (Internet Engineering Task Force (IETF) and the World Wide Web Consortium (W3C) etc)
- Private Sector Actors

In case of Nepal, Nepal Telecommunications Authority is generally responsible for governance of internet

#### 2.3 E-Governance and E-Government Systems

- E-governance is the use of technology to improve the efficiency, transparency, and accessibility of government services and information. Alternatively, process of providing government services and information to the following target group using technology:
  - G2C, G2B, G2E and G2G

19

### 2.3 E-Governance ...

- E-government systems mention to the specific technologies and platforms used to deliver these services and information
- These systems may have following benefits however it is important to ensure that these systems are designed and used with secured and confidential way to protect citizens' data and prevent cyber threats:
  - Online Service Delivery
  - Improved Transparency
  - Increased Accountability
  - Cost Savings
  - Accessibility

#### Components of E-governance:

- People
- Process
- Technology
- Resources

20

### 2.3 E-Governance ...

#### E-governance in Nepal a brief look:

- E-governance in Nepal refers to the use of information and communication technologies (ICTs) to improve the efficiency, transparency, and accountability of government services.
- The government of Nepal has been working to implement e-governance since the early 2000s, and has made significant progress in recent years through following bodies:
  - Ministry of Communications and Information Technology
  - E-governance Commission
  - National Information Technology Center (NITC)
  - Nepal Telecommunications Authority

21

#### 2.3 E-Governance ...in Nepal some glimpses from Nepali media..

काठमाडौं । सरकारी सेवालाई अनलाइनमार्फत प्रवाह गर्ने कार्यक्रममा समस्या नै समस्या रहेको महालेखा परीक्षकको कार्यालयले जनाएको छ । बिहीबार आफ्नो ६०औं वार्षिक प्रतिवेदनको सारांश सार्वजनिक गर्दै महालेखाले सरकारको अनलाइन सेवामा रहेका समस्या औल्याएको हो । जसमा सूचना प्रविधि साक्षरता तथा सुरक्षाको कमी रहेको र इन्टरनेटको पहुँच विस्तार हुन नसकेको जस्ता विषय समेत रहेका छन् ।

यस्तै विद्युतीय हस्ताक्षर प्रयोग हुन नसकेको, सूचना प्रविधि सम्बन्धी नीति नै नरहेको र सूचना प्रविधि प्रणालीलाई व्यवस्थित गर्न आवश्यक जनशक्ति अभाव रहेको लगायतका समस्या पनि महालेखाले औल्याएको छ ।

त्यसबाहेक तेस्रो पक्ष आश्वस्तता वा सूचना प्रविधि प्रणालीको लेखा परीक्षण हुन नसकेको, कोटा प्रणाली लागू गर्ने गरेको, सेवा अवरुद्ध भैरहने र भएको अवस्थामा वैकल्पिक व्यवस्था नभएको प्रतिवेदनमा उल्लेख छ ।

यसैगरी पूर्वाधारको कमी, निकायगत समन्वयको अभाव, सेवा प्राप्त गर्दा बाह्य पक्षको सहायता लिनुपर्ने अवस्था कायमै रहेको, फरक क्षमता भएका सेवाग्राहीका लागि विशेष व्यवस्था नभएको, सरकारी निकायमै विद्युतीय कागजातलाई मान्यता नदिएको लगायतका व्यहोरासमेत प्रतिवेदनले औल्याएको छ ।

22

• पछिल्लो अध्यावधिक: चैत ३०, २०७९

#### 2.3 E-Governance ...in Nepal some glimpses from Nepali media..

- सरकारले राष्ट्रिय सूचना तथा सञ्चार प्रविधि दिवस 'आइसिटी डे' आज मनाउने भएको छ । 'सुरक्षित सूचना प्रविधि, सुशासन र समृद्धि' भन्ने मूल नाराका साथ छैटौँ दिवस अर्थात् 'आइसिटी डे' यही वैशाख १७, १८ र १९ गते तीन दिनसम्म विभिन्न कार्यक्रम गरेर मनाउने भएको हो ।

दूरसञ्चार सेवाप्रदायकमार्फत तीन दिनसम्म वैशाख १७, १८ र १९ गते रिडब्याक टोनका रूपमा 'आईसीटी डे २०२३' भव्य रूपमा मनाउँँ भन्ने सन्देशका साथै वैशाख १९ गते बिहान मोबाइल प्रयोगकर्तालाई एसएमएसमार्फत पठाउने व्यवस्था मिलाउन नेपाल दूरसञ्चार प्राधिकरणलाई अनुरोध गर्ने प्रचार उपसमितिले जनाएको छ ।

यसै अवसरमा राष्ट्रिय साइबर सुरक्षा केन्द्र स्थापना गर्ने अध्ययन भइरहेको बताएका छन् । साइबर सुरक्षाको बढ्दो चुनौतीलाई मध्यनजर गर्दै आवश्यक नीति, नियम र सरचना बनाउने कार्यलाई सरकारले प्राथमिकता दिएको उनको भनाइ छ ।

नेपालमा २०२८ सालमा कम्प्युटर भित्रिएको थियो । नेपालमा कम्प्युटर एसोसिएसन नेपाल (क्यान)को सन् १९९२ मा स्थापना भयो । त्यही स्थापना भएको दिनलाई सूचना प्रविधि दिवसका रूपमा मनाउन थालेको हो ।

- एनपी सर्टको वेबसाइट सार्वजनिक, आईपी एड्रेसदेखि लिङ्कसम्म स्क्रान गर्न सकिने, २०८० वैशाख १९ गते

• Geoffrey Hinton, *The Godfather of A.I.' Leaves Google and Warns of Danger Ahead*, May 1, 2023

### 3. Computer Ethics and Ethical Theories

- The word "ethics" comes from an ancient Greek word *echē*, which means character, so is the philosophical study of **morality**. Alternatively, the study of what it means to "do the right thing."
- **Morality** is a set of principles of right conduct used to modify and regulate our behavior, applicable to all in a group or society and followed in our day-to-day living for the betterment of our lives. Further means to ethics, then **law**
- **Law** is a set of rules for defining correct procedure or behaviors to protect the life, liberty, and property of individual, group or society for improve our lives
- **Computer ethics** is the study of ethics related to use of computer technology, including the use of computers, software, and networks for the improvement of our lives
- **Why Should Study Computer Ethics?**

a study of computer ethics will equip us with those skills we need in our computer-directed professional lives as we solve those conflicts that we will definitely encounter

### 3. Computer Ethics...

- **Ethical theories** are the frameworks for understanding what is right or wrong, good or bad, and just or unjust
- There are many ethical theories such as Utilitarianism, deontology, relativism etc.

#### 3.1 Philosophical and Professional Ethics

- **Philosophical ethics** is a branch of philosophy that deals with questions about what is morally right or wrong, good or bad, just or unjust, and how we ought to live our lives on the basis of people, community, society, religion and nature
- **Professional ethics** is a set of principles and standards that guide the conduct and behavior of professionals in a particular field, typically include a code of conduct, which outlines the ethical standards and principles that professionals are expected to follow for fulfilling the responsibilities towards their clients, colleagues, and society
- Philosophical ethics provides a foundation for the development of professional ethics, and professional ethics provides a framework for the application of ethical principles in practice

### 3. Computer Ethics...

#### 3.2 Moral and Legal Issues

- Moral and legal issues refer to different but often interrelated aspects of human behavior and decision-making
- **Moral issues** pertain to questions of right and wrong, good and bad, and the principles and values that guide human conduct based on cultural, social, and personal beliefs. Eg. abortion, same-sex marriage, death penalty etc.
- **Legal issues** concern to questions of legality, justice, and compliance with the law. These issues are based on the existing legal framework in a particular jurisdiction and are usually governed by regulations, and judicial decisions. Eg. intellectual property rights, cyber law etc.

#### 3.3 Descriptive and Normative Claims

It is important to distinguish between descriptive and normative claims because they require different forms of evidence and argumentation.

**Descriptive claims** are subject to empirical investigation eg. "The sky is blue", while **normative claims** require ethical, philosophical, or political justification eg. "People should always tell the truth"

### 3. Computer Ethics...

#### 3.4 Ethical Relativism

- Ethical relativism is the view that moral values and principles are relative to a particular culture or society, and there is no objective or universal standard of morality that applies to all individuals and societies. i.e., consideration of right or wrong, good or bad, can vary depending on the culture or society. Eg. Use of beef as nonveg

#### 3.5 Utilitarianism and Deontological Theories

- **Utilitarianism** theory puts a group's interest and happiness above those of an individual, for the good of many, an action is good if it benefits the maximum number of people. In computer ethics, this may be applied to decisions about the use of technology that will have the greatest positive impact on society
- **Deontology** comes from two Greek words, deon meaning duty and logos meaning science. Hence, this theory has a duty attached to it and an act is considered good if the individual committing it had a good reason to do so and based on the idea that certain actions are inherently right or wrong, regardless of their consequences. In computer ethics, this may be used to guide decisions about privacy, security, and other ethical issues

### 3. Computer Ethics...

#### 3.6 Rights

Rights are the entitlements or permissions that individuals or groups of people have to act, think, or say certain things without interference or oppression from others. These can be legal, moral, or ethical in nature, and may be protected by various forms of law, convention, or social contract. Some of the rights are:

- Human rights
- Civil rights
- Legal rights
- Moral rights
- Natural rights
- Copy rights

28

### 4. Professional Ethics

- **Professional ethics** is a set of rules, principles and standards in a particular field that includes relationships as well as behaviors with and responsibilities toward customers, clients, coworkers, employees, employers, people who use one's products and services, others whom one's products affect and society
- Contain various aspects such as *profession, professional responsibilities and rights, professional code of ethics and hacker ethics and netiquette* etc.

#### 4.1 Profession

A **profession** is a vocation that requires a high level of education and practical experience in that field. Professionals have a special obligation to ensure their actions are for the good of those who depend on them, because their decisions can have more serious consequences than the choices made by those holding less responsible positions in society.<sup>29</sup>

### 4. Professional Ethics...

#### 4.1.1 Job and Occupation

**Job** is a full or part-time position of paid employment i.e., the regular work that a person does to earn money. A particular piece of work with responsibility.

**Occupation** is a general term that refers to the field you are a part of or the work you are interested in. It can also refer to your role within an organization.

A job title describes someone's specific duty or position, like "podiatrist," whereas an occupation refers to a broader title or the entire industry in which someone works, like "doctor."

30

#### 4. Professional Ethics...

##### 4.1.2 Characteristics of Profession

A profession is characterized by a commitment to excellence, a dedication to service, and a focus on advancing the knowledge and practice of the field. However, a profession has following characteristics:

- Specialized Knowledge
- Responsibility and Accountability
- Ethical Standards
- Autonomy
- Service Orientation
- Formal Credentialing
- Continuous Learning
- Professional Associations

31

#### 4. Professional Ethics...

##### 4.1.3 Engineering and Computing as a profession

Initially, a computer-related job, such as system administration, computer programming, or software engineering, is not considered as a full-fledged profession like medicine or law, because they do not need to be certified and licensed in order to design, implement, or maintain computer hardware or software. Nevertheless, those who work with computers can, through inadequate education, insufficient practical training, or bad choices, cause a great deal of harm.

In this respect, the realization of computer professionals must be similar to that of members of fully developed professions, the computing societies have worked together to develop a code of ethics to guide the actions of computer/software engineers: those who develop or maintain computer/software or teach in this area and succeed to move towards profession

As a result, engineering and computing are two of the most challenging and in-demand professions in the world today. Engineers and computer scientists are responsible for designing, developing, and maintaining the systems that we all rely on our daily life

#### 4. Professional Ethics...

##### 4.2 Professional Responsibilities and Rights

Professional responsibilities are the duties and rights are the entitlements that come with being a professional in a particular field.

By understanding responsibilities and rights, professionals can ensure the integrity and effectiveness of their work, as well as for protecting the public's as well themselves safety and well-being. These can vary depending on the profession but they typically include things like:

for professional responsibilities

- providing competent and ethical service
- protecting the confidentiality of clients
- abiding by the laws and regulations governing the profession

for professional rights

- the right to practice their profession
- the right to be compensated fairly
- the right to be protected from discrimination

#### 4. Professional Ethics...

##### 4.2.1 Conflict of Interests and Whistleblowing

A **conflict of interests** is a situation in which a person or organization is in a position to derive personal benefit from actions or decisions made by them or in their official capacity, can arise in a variety of settings, including business, government, and the nonprofit sector.

**Whistleblowing** is the act of reporting unethical, illegal, or unsafe practices by an individual or organization to the appropriate authorities or public. Whistleblowers often face retaliation for their actions, but they can play a critical role in promoting transparency and accountability in organizations.

Many countries have their own laws and regulations to protect whistleblowers from retaliation. In the Nepal also we have, for example

- The Public Interest Disclosure Act, 2064 (2007): This law provides protection for public servants who report wrongdoing to the appropriate authorities.
- The Corruption Prevention Act, 2062 (2005): This law provides protection for anyone who reports corruption to the appropriate authorities.
- The Anti-Money Laundering Act, 2064 (2007): This law provides protection for anyone who reports money laundering to the appropriate authorities.

#### 4. Professional Ethics...

##### 4.3 Professional Code of ethics

Many professional organizations have codes of professional conduct to provide a general statement of ethical values and remind people in the profession that ethical behavior is an essential part of their job as well as field specific professional responsibilities

They provide valuable guidance for new or young members of the profession who want to behave ethically but do not know what is expected of them, people whose limited experience has not prepared them to be alert to difficult ethical situations and to handle them appropriately

There are several organizations for the range of **Professional Code of ethics** however we have a discussion on **Code of ethics of Nepal Engineering Council** and **Code of Ethics of IEEE and ACM**:

#### 4.3 Professional Code of ethics...

##### 4.3.1 Code of ethics of Nepal Engineering Council

The professional Code of Conduct to be followed by the registered Engineers of the Council, subject to the provision of the Nepal Engineering Council (NEC) Act, 2055 (1998) and the Nepal Engineering Council Regulation, 2057(2000), has been published as follows:

**1. Discipline and Honesty:** The Engineering service/profession must be conducted in a disciplined manner with honesty, not contravening professional dignity and well-being.

**2. Politeness and Confidentiality:** Engineering services for customers should be dealt with in a polite manner and professional information should remain confidential except with written or verbal consent of the customers concerned. This, however, is not deemed to be a restriction to provide such information to the concerned authority as per the existing laws.

**3. Non-discrimination:** No discrimination should be made against customers on the grounds of religion, race, sex, caste or any other things while applying professional knowledge and skills.



#### 4.3.1 Code of ethics of Nepal Engineering Council...

**4. Professional Work:** Individuals should only do professional work in their field or provide recommendations or suggestions only within the area of their subject of study or obtained knowledge or skills. With regard to the works not falling within the subject of one's profession, such works should be recommended to be done by an expert of that subject matter.

**5. Deeds which may cause harm to the engineering profession:** With the exception of salary, allowance and benefits to be received for services provided, one shall not obtain improper financial gain of any kind or conduct improper activities of any kind, which would impair the engineering profession.

**6. Personal responsibility:** All individuals will be personally responsible for all works performed in connection with his/her engineering profession.

#### 4.3.1 Code of ethics of Nepal Engineering Council...

**7. State name, designation and registration no:** While signing the documents or descriptions such as the design, map, specifications and estimates etc, relating to the engineering profession, the details should include, the name, designation and NEC registration No. and should be stated in a clear and comprehensible manner.

**8. No publicity or advertisement must be made which may cause unnecessary effect:** In connection with the professional activities to be carried out, no publicity or advertisement shall be made so as to cause unnecessary effect upon the customers.

*Note: Engineers, working with government, quasi government, private sectors, NGOs, INGOs, bilateral and multilateral agencies and consultants etc., if not registered with NEC, can be punished as it would be against the Law of Land. NEC is not responsible for registering engineers who complete their studies from any institute or through any engineering programs unless and until such programs are inspected/monitored & approved by NEC.*

#### 4.3.1 Code of ethics of Nepal Engineering Council...



##### Nepal Engineering Council Professional Code of Conduct

The professional Code of Conduct to be followed by the registered Engineers of the Council, subject to the provision of the Nepal Engineering Council (NEC) Act, 2055 (1998) and the Nepal Engineering Council Regulation, 2057(2000), has been published as follows:

- Discipline and Honesty:** The Engineering service/profession must be conducted in a disciplined manner with honesty, not contravening professional dignity and well-being.
- Politeness and Confidentiality:** Engineering services for customers should be dealt with in a polite manner and professional information should remain confidential except with written or verbal consent of the customers concerned. This, however, is not deemed to be a restriction to provide such information to the concerned authority as per the existing laws.
- Non-discrimination:** No discrimination should be made against customers on the grounds of religion, race, sex, caste or any other things while applying professional knowledge and skills.
- Professional Work:** Individuals should only do professional work in their field or provide recommendations or suggestions only within the area of their subject of study or obtained knowledge or skills. With regard to the works not falling within the subject of one's profession, such works should be recommended to be done by an expert of that subject matter.
- Deeds which may cause harm to the engineering profession:** With the exception of salary, allowance and benefits to be received for services provided, one shall not obtain improper financial gain of any kind or conduct improper activities of any kind, which would impair the engineering profession.
- Personal responsibility:** All individuals will be personally responsible for all works performed in connection with his/her engineering profession.
- State name, designation and registration no:** While signing the documents or descriptions such as the design, map, specifications and estimates etc, relating to the engineering profession, the details should include, the name, designation and NEC registration No. and should be stated in a clear and comprehensible manner.
- No publicity or advertisement must be made which may cause unnecessary effect:** In connection with the professional activities to be carried out, no publicity or advertisement shall be made so as to cause unnecessary effect upon the customers.

*Note: Engineers, working with government, quasi government, private sectors, NGOs, INGOs, bilateral and multilateral agencies and consultants etc., if not registered with NEC, can be punished as it would be against the Law of Land.  
NEC is not responsible for registering engineers who complete their studies from any institute or through any engineering programs unless and until such programs are inspected/monitored & approved by NEC.*

Nepal Engineering Council  
Bhagwati Marg 742/4, Nawal, Kathmandu - 1  
Post Box No. 2049, Phone No. 977-01-4420655, 4420656  
Fax: 977-01-4422099  
Website: [www.nec.gov.np](http://www.nec.gov.np), Email: [necgov@nec.net.np](mailto:necgov@nec.net.np)

#### 4.3 Professional Code of ethics...

##### 4.3.2 Code of Ethics of IEEE and ACM

##### Code of Ethics of IEEE

The code of ethics of IEEE approved by the IEEE Board of Directors February 2006 is:

We, the members of the IEEE, in recognition of the importance of our technologies in affecting the quality of life throughout the world and in accepting a personal obligation to our profession, its members and the communities we serve, do hereby commit ourselves to the highest ethical and professional conduct and agree:

##### IEEE CODE OF ETHICS

- To accept responsibility in making decisions consistent with the safety, health and welfare of the public, and to disclose promptly factors that might endanger the public or the environment;
- To avoid real or perceived conflicts of interest whenever possible, and to disclose them to affected parties when they do exist;
- To be honest and realistic in stating claims or estimates based on available data;

#### Code of Ethics of IEEE ...

- To reject bribery in all its forms;
- To improve the understanding of technology, its appropriate application, and potential consequences;
- To maintain and improve our technical competence and to undertake technological tasks for others only if qualified by training or experience, or after full disclosure of pertinent limitations;
- To seek, accept, and offer honest criticism of technical work, to acknowledge and correct errors, and to credit properly the contributions of others;
- To treat fairly all persons regardless of such factors as race, religion, gender, disability, age, or national origin;
- To avoid injuring others, their property, reputation, or employment by false or malicious action;
- To assist colleagues and co-workers in their professional development and to support them in following this code of ethics.

#### 4.3.2 Code of Ethics of IEEE and ACM...

##### Code of Ethics of ACM

##### ACM Code of Ethics and Professional Conduct

Adopted by ACM Council 10/16/92.

##### 1. GENERAL MORAL IMPERATIVES

As an ACM member I will ....

------(8)

##### 2. MORE SPECIFIC PROFESSIONAL RESPONSIBILITIES

As an ACM computing professional, I will ....

------(8)

##### 3. ORGANIZATIONAL LEADERSHIP IMPERATIVES

As an ACM member and an organizational leader, I will ....

------(6)

##### 4. COMPLIANCE WITH THE CODE

As an ACM member I will ....

------(2)

## 4. Professional Ethics...

### 4.4 Hacker ethics and Netiquette

- **Hack/Hacking** is the act of identifying and then exploiting weaknesses in a computer system or network, usually to gain unauthorized access to personal or organizational data. Hacking is not always a malicious activity, *the notion of the "hack" is a "neat" technological trick and the idea of playfulness*, but the term has mostly negative connotations due to its association with cybercrime
- A **hacker** is an individual who uses computer, networking or other skills to overcome a technical problem. The term also may refer to anyone who uses their abilities to gain unauthorized access to systems or networks in order to commit crimes

Richard Stallman describes:

- The **hacker ethic** refers to the feelings of right and wrong, to the ethical ideas this community of people had—that knowledge should be shared with other people who can benefit from it, and that important resources should be utilized rather than wasted

### 4.4 Hacker ethics and Netiquette...

#### Hacker ethics...

The hacker ethic is a philosophy and set of moral values as well as principles that guide the behavior of ethical hackers to use their technical skills for identify weaknesses in computer systems and networks in order to help organizations improve their security and are may be:

- Access to computers should be unlimited and total
- All information should be free
- Mistrust authority
- Contribute to the community
- Protect the innocent
- Have fun

#### Netiquette

Netiquette is a made-up word from the words net and etiquette. Netiquette thus describes the rules of conduct for respectful and appropriate communication on the internet

### 4.4 Hacker ethics and Netiquette...

#### Netiquette...

Thus, "Netiquette" is network etiquette for the do's and don'ts of online communication. Netiquette covers both common courtesy online and the informal "rules of the road" of cyberspace, such as:

- Rule 1: Remember the Human
- Rule 2: Adhere to the same standards of behavior online that you follow in real life
- Rule 3: Know where you are in cyberspace
- Rule 4: Respect other people's time and bandwidth
- Rule 5: Make yourself look good online
- Rule 6: Share expert knowledge
- Rule 7: Help keep flame wars under control
- Rule 8: Respect other people's privacy
- Rule 9: Don't abuse your power
- Rule 10: Be forgiving of other people's mistakes

## 5. Risk and Responsibilities

- **Risk** characterized as **uncertainty and/or loss** is the possibility of harm or loss occurring as a result of a particular decision or action
- **Responsibility** is the obligation or duty to take care of something or someone while making decision or taking action in order to minimize harm or loss
- Responsibility helps to minimize or manage risks, hence Risk and responsibility are connected to each other these are two closely related concepts
- IT is a complex and ever-changing field containing number of risks and responsibilities such as *computer liability, values in design, professional responsibilities of computer users* etc.
- By understanding these, we can help to protect ourselves, our organizations, our communities and further help to use these technologies for the betterment of our lives

## 5. Risk and...

### 5.1 Computer Liability

- A legal term that represents the responsibility as well as accountability of digital technology users (individuals or organizations) and developers
- May include issues related to data privacy, security holes, defamation and other legal violations such as *malfunction of computers, safety in critical systems, accuracy vs. democracy in internet, misinterpretation of information and its liability* etc.
- Eg., if an organization's computer system is hacked, resulting in the theft or loss of customer data, the organization may be held liable for damages resulting from that problem

### 5.1 Computer Liability...

#### 5.1.1 Malfunction of Computers

- An error or defect, especially in a computer system (i.e. hardware, software and network) cause the entire system to stop working properly
- There are different types of computer malfunctions caused by a variety of factors and are:
  - *Hardware failure*: stops working by physical components such as the hard drive, motherboard, or graphics card caused by overheating, physical damage, or manufacturing defects etc
  - *Software malfunction*: stop working properly by software program such as operating system. application s/w or a driver caused by bugs, viruses, user error etc
  - *Network problems*: problem due to computer's network connection caused by faulty network card, a bad cable, or a problem with the router etc.
  - *User error*: problem due to user does something wrong result in computer to malfunction caused by installing the wrong software, deleting important files, or accidentally turning off the computer etc.



## 5.1 Computer Liability...

### 5.1.2 Safety in Critical Systems

- Indicates safety of those systems whose failure or malfunction could result in harm or injury to humans, damage to property, or severe several environmental as well as social damages, such as:
  - Air traffic control systems
  - Nuclear power plants
  - Medical devices
  - Automobiles
  - Automated manufacturing systems
- It is a critical concern for all stakeholders, including system developers, users, and regulators and hence, achieved through a combination of engineering design, testing, and operational procedures which need several measures, these measures include:

49

## 5.1.2 Safety in Critical Systems...

- Risk Assessment: A thorough risk assessment is necessary to identify potential hazards and their likelihood of occurrence such as analyzing the system's design, operation, and maintenance procedures, as well as any external factors that may impact the system
- Safety Standards: Compliance with safety standards such as ISO 26262 for automotive systems, DO-178B/C for avionics systems, and IEC 61508 for general-purpose systems etc.
- Redundancy and Diversity: Incorporate redundancy and diversity to ensure that if one component fails, the system can continue to operate. Redundancy means having backup components that can take over in the event of a failure, while diversity means using different types of components to minimize the chance of a common mode failure.

50

## 5.1 Computer Liability...

### 5.1.2 Safety in Critical Systems...

- Testing and Verification: Testing and verification of systems is necessary to ensure that they meet objective and safety requirements. This includes both software and hardware testing, and may involve simulation, prototyping, and real-world testing
- Maintenance and Monitoring: Regular maintenance and monitoring of critical systems is essential to ensure that they continue to operate safely. This includes preventative maintenance, periodic inspections, and monitoring of system performance.

### 5.1.3 Accuracy vs. Democracy in Internet

- The internet has had a profound impact on society. It has made easier for people to access information. However, it has challenges to provide access to this technology rapidly continues to become more accessible to more people (**democracy in internet**) on the one hand and the accuracy of the information available on this technology on the other hand.
- Inaccuracy of information results in misinformation is false or misleading information that is spread intentionally or unintentionally in internet. It can be spread through social media, news websites, and even through government as well as other relevant websites. Misinformation can have a misunderstanding, as well as negative impact on society

## 5.1 Computer Liability...

### 5.1.4 Misinterpretation of Information and its Liability

- Misinterpretation of information is another major problem of digital technology. Misinterpretation of information can lead to a number of negative consequences such as decision-making errors, conflict, spread of misinformation, loss of trust etc. and it may be intentionally or unintentionally.
- In some cases, misinterpretation of information can also lead to legal liability. However, liability for misinterpretation of information is not always clear-cut. In some cases, it may be difficult to prove that the misinformation was the direct cause of harm or loss. Additionally, there may be factors such as disclaimers or limitations of liability that could limit or negate any legal liability.

52

## 5.2 Values in Design

- Values in design are important in invention because they provide a framework for designer to create products and services that better serve the needs of users and society which also promoting ethical and sustainable practices
- Every now and then, invention or technology who become more successful and sustainable most often based on society's basic sets of moral values however many are do not last for more than a month; others are disappears and collapses
- The values that are important to a designer will vary depending on the project or technology such as software and hardware design may have different values

### 5.2.1 Software and Design Problems

Design problems are a common characteristic of software development process/industry, they can include a wide range of issues that can arise during the development and implementation of software such as:

## 5.2.1 Software and Design Problems...

- Bugs and errors: Issues that prevent software from functioning correctly or as intended and may occur due to coding mistakes, incorrect logic, or other factors
- Performance issues: These are problems that affect the speed or responsiveness of software, such as slow load times, lags, or crashes.
- Usability issues: These are problems that make software difficult to use or navigate, such as confusing interfaces, unclear instructions, or poorly organized information
- Security vulnerabilities: These are weaknesses in software that can be exploited by hackers or other malicious actors to gain unauthorized access to sensitive data or systems
- Compatibility issues: These are problems that arise when software is not compatible with other hardware or software systems, such as operating systems or web browsers
- Design problems: These are issues related to the design and user experience of software, such as poor color schemes, cluttered layouts, or inadequate feedback mechanisms

These problems may be addressed by careful planning, testing, and troubleshooting throughout the software development process which may involve collaboration with other stakeholders such as users, designers, and security experts

54

### 5.2.2 Hardware Design Issue

## 5.2 Values in Design...

Hardware design is a complex process of developing a physical product from a conceptual design may include a number of issues and are:

- Requirements gathering: This is the process of understanding the needs of the users and stakeholders.
- Conceptual design: This is the process of developing a high-level overview of the product, including its features, functionality, and user interface.
- Detailed design: This is the process of developing a detailed specification of the product, including its components, layout, and manufacturing processes.
- Testing: This is the process of verifying that the product meets its requirements.
- Manufacturing: This is the process of producing the product in large quantities.

However, hardware design for digital equipment may include technical issues such as Power and thermal management, Signal integrity, Electromagnetic interference (EMI), Timing and synchronization, and notion of users etc.

## 5.2 Values in Design...

### 5.2.3 Elimination of Hardware

Elimination of hardware is the process of reducing or completely removing physical components or devices from a system or environment, often in favor of software-based alternatives. The goal of eliminating hardware is typically to reduce costs, increase efficiency, and simplify maintenance and management.

Eg. Use of cloud-based technology instead of physical server

### 5.3 Professional Responsibilities of Computer Users

Professional responsibilities of computer users ensure that the user using computers in a responsible, accountable and ethical manner and, contribute to a safe and secure computing environment, for this following guidelines may play key roles:

- Using computers in a responsible and ethical manner
- Protecting computer systems and data from unauthorized access, use, or disclosure
- Reporting any security breaches or suspicious activity to your IT department immediately
- Keeping your computer skills up to date
- Being a good role model for others

56

### 5.3 Professional Responsibilities of Computer Users...

#### 5.3.1 Responsibility and Accountability

**Responsibility** is the commitment to do something. It is the duty or expectation that someone will fulfill a task or role. **Accountability** is the commitment to report to someone or to be answerable for one's actions. It is the expectation that someone will be held responsible for their decisions and actions.

Hence, responsibility and accountability are two closely related but distinct concepts, it is important to foster a culture of responsibility and accountability for individuals and organizations to create a successful workplace

- For computer users:

They have a responsibility to use computers in a responsible and ethical manner. This means using them for legitimate purposes, not for illegal or unethical activities. It also means respecting the privacy of others and not using their computers without their permission.

They are also accountable for their actions on computers. This means that they can be held responsible for any damage or harm that they cause, either intentionally or unintentionally. For example, if a computer user installs a virus on a company computer, they could be held liable for the cost of repairs or lost productivity.

### 5.3 Professional Responsibilities of Computer Users...

#### 5.3.1 Responsibility and Accountability

**Responsibility** is the commitment to do something. It is the duty or expectation that someone will fulfill a task or role. **Accountability** is the commitment to report to someone or to be answerable for one's actions. It is the expectation that someone will be held responsible for their decisions and actions.

Hence, responsibility and accountability are two closely related but distinct concepts, it is important to foster a culture of responsibility and accountability for individuals and organizations to create a successful workplace

- For computer users:

They have a responsibility to use computers in a responsible and ethical manner. This means using them for legitimate purposes, not for illegal or unethical activities. It also means respecting the privacy of others and not using their computers without their permission.

They are also accountable for their actions on computers. This means that they can be held responsible for any damage or harm that they cause, either intentionally or unintentionally. For example, if a computer user installs a virus on a company computer, they could be held liable for the cost of repairs or lost productivity.

### Case Study Examples

1. You are asking to write a program to print tags for a sale. Your boss asks you to put tags that have a price 10% higher, with a 10% discount marking it back to original price. Are you going to do this? What ethical theory you are going to apply?

2. You contracted to install Netscape Navigator software on all the PCs of company X. After doing half the work, you found that company X is not paying Netscape for the copies you are installing. You notified company X's contact that they are out of compliance with Netscape licensing requirement, but got no response. What ethical theory are you going to apply based in your action?

Solution:

1. Deontology or ethical egoism (ethical egoism, in philosophy, an ethical theory according to which moral decision making should be guided entirely by self-interest) is the belief which guide to do this task.
2. Descriptive ethics, that branch of ethics concerned with criteria of empirical investigation, on the basis of contract.

### Case Study Examples

#### 3. Read the following case study and answer the questions at the end.

**Digital Data Divide (DDD)** is a small IT outsourcing enterprise. It was founded in 2001 with the aim of helping youths coming from not having very financially sound backgrounds, lacking resources or have any other disabilities to get job opportunities in the IT sector. The company wants to do this by providing computer and English classes to them and further offering them jobs or promotions after these training sessions. The business goal of DDD is to provide opportunities for getting into the IT sector to people who are facing poverty, lacking resources, or have any other disabilities.

Since the business is a social enterprise operating on a small scale, it is facing some financial and HR issues. The main problem is that there are many other IT firms present in the market so the youths trained by DDD are going to its competitors for jobs as they are offering higher salaries. This has led to an employee shortage crisis for the company. Keeping in mind all these challenges, the main strategic choice in front of DDD is whether it should expand or merge with any other similar firm to address the financial problems it is facing.

Also, the company has to decide on the right business model for its expansion because its main mission is social good so it must be ensured that the expansion does not restrict or hinders this mission and DDD successfully achieves its goal.

1. What is DDD? Explain with its business goal.
2. What type of HR and financial issues are facing DDD?
3. What are the possible solutions to the problems facing DDD?
4. Do you think DDD is suitable in Nepal?

60

### Case Study Examples

#### Digital Data Divide (DDD) Solutions:

1. Digital Data Divide (DDD) is a small IT outsourcing enterprise with business goal to provide opportunities for getting into the IT sector to people who are facing poverty, lacking resources, or have any other disabilities.
2. The main HR issue facing DDD is that the youths trained by DDD are going to its competitors for jobs as they are offering higher salaries. This has led to an employee shortage crisis for the company which further results in facing financial problems and the company is also facing competition from other IT firms.
3. Some possible solutions to the problems facing DDD are:
  - Increasing salaries to attract and retain employees.
  - Expanding into new markets.
  - Merging with another similar firm.
  - Developing a new business model.
4. Yes, DDD is suitable in Nepal. Nepal is a developing country with a large population of young people. Many of these young people are looking for opportunities to improve their lives and to contribute to the development of their country. DDD can provide these opportunities by providing training and employment in the IT sector and help to address the digital divide in country. 61

### Case Study Examples

#### 4. Read the passage and answer the questions that follow:

Around 2000, The Atlantic Monthly and other publications revealed a distinct issue: The Internet allows people who exhibit or wish to practice abnormal behavior to find one another easily, due to anonymous search engines and online forums or services. As sparse subpopulations, it was often unlikely or difficult to find willing partners or like-minded individuals prior to the Internet.

A small number of these subcultures promote self-destructive or mutually destructive behavior. Websites and mailing lists exist that explicitly promote anorexia, apotemnophilia, necrophilia, and suicide. While these activities are easily recognized as abnormal and self-destructive by most adults, many people fear that children or mentally ill persons visiting such sites would lack the maturity necessary to make that discrimination.

In rare cases, people have used the Internet to find willing partners for abnormal activities, but with disastrous or fatal results. In one case, a German named Armin Meiwes (the "German cannibal") made an online arrangement with Bernd Jurgen Armando Brandes to kill and eat him. Meiwes was later convicted of manslaughter.

1. What do you conclude from the above passage?
2. Do you think this kind of issue can be highly sensitive for minors? How?
3. What are the possible solutions that you see to the above problem?
4. What are some of the major impacts of Internet you have seen in Nepal?

62

## 6. Privacy

- The word privacy is derived from the Latin word "privatus" which means set apart from what is public, personal and belonging to oneself, and not to the state
- Privacy revolve around the notion of access, where access means either physical proximity to a person or knowledge about that person but society can be harmed if individuals have too much privacy. Hence, it is difficult where to draw the line between what is private and what is public
- However, privacy is a social arrangement that allows individuals to have some level of control over who is able to gain access to their physical selves and their personal information to maintain and develop socio-structure, society and nation. Hence, the **Constitution** of each country also guaranteed the right to privacy
- In our country, **The Constitution of Nepal** guarantees the right to privacy. Article 17(1) states that "No person shall be subjected to interference with his privacy, home or correspondence."
- It would seem that privacy is not a simple concept, however to understand privacy a discussion is made here on various aspects such as **Privacy and its Value, Privacy Risks, Privacy of Consumer Information, Protecting Privacy, Offensive Speech and Censorship in Cyberspace, Anonymity etc.**

## 6. Privacy...

### 6.1 Privacy and its Value

There is a tug-of-war between the desires, rights, and responsibilities of a person who wants to restrict access to himself or herself, and the desires, rights, and responsibilities of outsiders to gain access.

Privacy has traditionally been perceived as valuable because it lets us be ourselves and has even gained more importance in the digital age because it guards an individual's *personal identity*, *preserves individual autonomy*, and makes *social relationships* possible.

### 6.2 Privacy Risks

Socialization and individuation are both necessary steps for a person to reach maturity. Privacy is necessary for a person to blossom as an individual. However, it is difficult to maintain complete privacy.

### 6.2 Privacy Risks...

This is an age of information technology, where computers, the Internet, and a whole array of digital devices—with their astounding increases in speed, storage space, and connectivity—make the collection, searching, analysis, storage, access, and distribution of huge amounts of information and images much easier, cheaper, and faster than ever before. These are great benefits. But when the information is about us, the same capabilities threaten our privacy as **unauthorized access, use, disclosure, disruption, modification, or destruction**, hence has made new threats possible and old threats more potent due to *Human error, Technical vulnerabilities Malicious actors and Regulatory changes* etc.

The privacy risks can vary depending on the type of information, the number of people, and the laws and regulations that apply such as **government information** and **consumer information** may have different privacy risks.

65

## 6.2 Privacy Risks...

### 6.2.1 Government Information

Federal and local government agencies maintain thousands of databases containing personal information. Examples include tax, property ownership, medical, travel, divorce, voter registration, bankruptcy, and arrest records. Others include applications for government grant and loan programs, professional and trade licenses, and school records (including psychological testing of children). And there are many, many more.

Government databases help government agencies perform their functions, determine eligibility for government benefits programs, detect fraud in government programs, collect taxes, and catch people who are breaking laws. The scope of government activities is enormous, ranging from catching violent criminals to licensing flower arrangers. Governments can arrest people, jail them, and seize assets from them.

Thus, the use and misuse of personal data by government agencies pose special threats to liberty and personal privacy. It seems reasonable to expect governments to meet an especially high standard for privacy protection and adherence to their rules.

## 6.2 Privacy Risks...

### 6.2.2 Consumer Information

A **consumer** is a person or a group who intends to order, or uses purchased goods, products, or services primarily for personal, social, family, household and similar needs.

"Consumer information" is considered to be "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report." This would include "information that results in whole or in part from manipulation of information taken from a consumer report, and information that has been combined with other types of information."

In other word, Consumer information is any information that is collected about a consumer, such as their name, address, phone number, email address, purchase history, and browsing habits by the businesses, governments, or other organizations while a consumer intends to order, or uses purchased goods, products, or services from them, in order to provide better services. However, the use and misuse of those information by the organization pose special threats to liberty and personal privacy.

## 6. Privacy...

### 6.3 Privacy of Consumer Information

Consumer information is a valuable asset for businesses or organizations. It can be used to target marketing campaigns, prevent fraud, improve customer service, and conduct research for the further improvement.

However, consumer information is also a valuable target for cybercriminals. If this information is compromised, it can lead to identity theft, financial loss, and emotional distress. Thus, it is necessary to maintain privacy against unauthorized access, use, disclosure, disruption, modification, or destruction of consumer information for which maintaining of followings may have key role:

#### 6.3.1 Databases and Personal Records

Database is a collection and organization of data in order to easy access, manage, and update. Personal records are any records that contain personal information about an individual, such as their name, address, phone number, email address, date of birth, Social Security number etc.

## 6.3 Privacy of Consumer Information...

### 6.3.1 Databases and Personal Records...

These (Databases and personal records) are often used together to store and manage personal information. Such as consumer information, employee information. This information could then be used to meet the objective of the organization as well its further improvement.

However, there is a chance of misuses and unauthorized access of such information this necessitates being careful and make sur to use of privacy guidelines as well as settings.

#### 6.3.2 E-mail Privacy

Email privacy dealing with issues of unauthorized access to, and inspection of, electronic mail, or unauthorized tracking when a user reads an email. This unauthorized access can happen while an email is in transit, as well as when it is stored on email servers or on a user's computer, or when the user reads the message.

E-mail privacy is necessary to maintain privacy of information such as the sender's and recipient's names, email addresses, and the contents of the email against unauthorized in order to secured from fraud and other crimes, this necessitates being aware of risk of using this technology and, make sure to use of privacy settings.

## 6. Privacy...

### 6.3 Privacy of Consumer Information... 6.3.3 Web Privacy

Web privacy is the prevention of personal information from unauthorized access and further includes security of computer systems from misdirecting or disrupting the services as well as information they are designed to provide.

In order to maintain web privacy, it is necessary to know about the risks of using this technology and, make sure to use of privacy settings while using this technology.

#### 6.4 Protecting Privacy

As computer or digital technology makes giant strides, better methods of information gathering are appearing every day; unfortunately, it seems that with such methods and techniques, individual privacy is under attack from individual, corporations, organizations, governments and businesses that have the means. Because individuals are outgunned by large corporations in their crusade for information, law-abiding individuals are forced to give up some of their rights in order to protect individual privacy.

## 6.4 Protecting Privacy...

However, many individuals, organizations, and businesses help meet the demand for privacy to some degree: Individual programmers post free privacy-protecting software on the Web. Entrepreneurs build new companies to provide technology-based privacy protections. Large businesses respond to consumer demand and improve policies and services. Organizations such as the Privacy Rights Clearinghouse provide excellent information resources. Activist organizations such as the Electronic Privacy Information Center inform the public, file lawsuits, and advocate for better privacy protection.

In this respect, to protect privacy, governments around the world have enacted laws and are enforcing these laws in courts. In Nepal, the government of Nepal has also issued a number of laws and guidelines on the privacy issues. These include:

- The Information Technology Act, 2063: The Information Technology Act, 2063 (2006) regulates the use of information technology in Nepal. Section 32 of the Act prohibits the collection, use, or disclosure of personal information without the consent of the individual.

71

## 6.4 Protecting Privacy...

- The Right to Information Act, 2064: The Right to Information Act, 2064 (2007) gives citizens the right to access information held by government agencies. However, the Act also allows government agencies to withhold information that is considered to be a "state secret" or that could harm the national interest.
- The Government of Nepal Guidelines on the Protection of Personal Information, 2014: These guidelines provide guidance to government agencies on how to collect, use, and disclose personal information in a way that protects the privacy of individuals.
- The Government of Nepal Guidelines on the Use of Information Technology in Government, 2015: These guidelines provide guidance to government agencies on how to use information technology in a way that protects the privacy of individuals.

## Privacy...

### 6.5 Offensive Speech and Censorship in Cyberspace

**Offensive speech**, is speech or form of communication that attacks or harm a person or group on the basis of attributes such as gender, ethnic origin, religion, race, disability, or sexual orientation, is a problem that has existed for centuries, but it has taken on new dimensions in the age of digital technology or cyberspace.

There are a number of reasons why offensive speech is a problem in cyberspace. First, it can create a hostile and intimidating environment for people who are targeted by it. Second, it can lead to violence and discrimination. Third, it can undermine the free flow of information and ideas.

73

## 6.5 Offensive Speech and Censorship in Cyberspace...

**Censorship in cyberspace** is the control or suppression of information that is disseminated through the internet. It can be carried out by governments, corporations, or individuals. Censorship can take many forms, including blocking websites, filtering content, and deleting posts. There are a number of reasons why censorship is carried out in cyberspace. Governments may censor information to protect national security, to promote a particular ideology, or to suppress dissent.

Censorship may be a major approach to dealing with offensive speech in cyberspace. However, censorship is a complex issue with no easy answers. On the one hand, censorship can help to protect people from being exposed to offensive speech. On the other hand, censorship can also be used to suppress dissent and limit the free flow of information.

74

## Privacy...

### 6.6 Anonymity

Anonymity is derived from the Greek word *anonymia*, meaning "without a name" or "namelessness". Hence, anonymity is the absence of identity. In the context of communication, anonymity refers to the ability to communicate without revealing one's identity, may become useful for today's information age to maintain privacy.

However, this concept may use in criminal and antisocial activities also.

75

## 7. Computer and Cyber Crimes

### 7.1 Introduction

Computer crimes and cybercrimes are related to each other and are often used interchangeably these are used to describe criminal activities that involve the use of computers or digital technologies such as computer hardware, software, network, internet etc. There are a lot of overlap between computer crimes and cybercrimes and very difficult to create boundary between them, however:

- **Computer Crime** is any illegal activity that is committed using a computer or targeting a computer system. It involves the unauthorized access, use, or manipulation of computer resources and data such as identity theft, unauthorized data access, and computer fraud etc. where individuals may involve.
- **Cyber Crime cyberspace** (online world) crime is a criminal activity conducted over the internet or other digital networks. It involves computer crimes, but it also covers activities like online scams, phishing, cyberstalking, online harassment, ransomware attacks, denial of service (DoS) attacks, data breaches, hacking, spreading malware or viruses etc. where individuals or organizations may involve and have a much wider impact, as they can affect millions of people at once

## 7.2 Types of Computer Crimes and/or Cyber-crimes

There are a numerous type of Computer Crimes/Cyber-crimes, it involves all crimes or criminal activities due to use of computers (hardware/ software), mobile devices internet (all activities related to online world social media) and other related digital devices as well as technologies etc., some of them are:

### 7.2.1 Traditional Computer Crimes and Software Piracy

- The earliest **computer crimes** were characterized as non-technological where theft of computer components, counterfeiting, digital/software piracy and copyright infringement were particular favorites. Later moved towards hacking, child pornography etc. Due to advent of technology, there were vast changes in this area and come up to this fearful, unsecured and threatened environment.
- **Software piracy** describes the acts of illegally copying, distribution, sharing, selling or using of software without ownership or legal rights whether intentional or not and results in a number of negative consequences such as financial losses, job losses, security risks, legal problems etc.

## 7.2 Types of Computer Crimes...

### Software piracy...

Software piracy is a major problem all over the world including Nepal. According to a 2019 study by the Business Software Alliance (BSA), the country's (Nepal's) software piracy rate is 75%. This means that for every 100 software programs used in Nepal, 75 of them are pirated. However, the government of Nepal has taken some steps to address the problem of software piracy. In 2010, the government passed the Copyright Act, which criminalizes software piracy. The government has also established a Copyright Enforcement Unit, which is responsible for investigating and prosecuting cases of software piracy.

### 7.2.2 Computer Frauds and Digital Forgery

**Computer fraud** is an act of using a computer to take or alter electronic data, or to gain unlawful use of a computer or system for unauthorized accessing computers, personal information and engaging in malware as well as hacking to disclose, alter, destroy information or system etc.

**Digital forgery** is the act of creating or altering digital data in a way that is intended to same as that of genuine using digital deceives as well as technologies such as...



## 7.2 Types of Computer Crimes...

### Computer Frauds and Digital Forgery...

- Creating fake documents, such as passports, birth certificates, or diplomas
- Altering existing documents, such as contracts or financial statements
- Creating or altering digital images or videos

In recent years, there has been a growing trend of these problems all over the world including Nepal as a result governments of different countries are taking steps to address this issue.

The government of Nepal is also taking steps to address this issue, such as passing the IT Policy 2067, Electronic Transactions Act 2063 (ETA), establishing the Cyber Crime Investigation Unit (CCIU) under the Nepal Police. However, needs to be done more in this area.

## 7.2 Types of Computer Crimes...

### 7.2.3 Phishing

A phishing (pronounced “fishing”) is an attack with a large-scale effort to gain sensitive information from **gullible computer users**. An attacker sends out millions of email messages from a **botnet** (a network of computers infected by malware that are under the control of a single attacking party). The messages inform the recipients that one of their accounts has been compromised and directs them to connect to a Web site to resolve the problem. Targeted users that click on the link encounter an impostor Web site designed to resemble the genuine ecommerce site. Once on the site, they are asked for a login name, password, and other private information. Information collected by the imposter site can then be used for identity theft. However, text messages, or phone calls are also used.

## 7.2 Types of Computer Crimes...

### 7.2.4 Unauthorized access: Hacking, cracking

An **unauthorized access** is a gaining of logical or physical access without permission to a network, system, application, data, or other resources using tactics like hacking, cracking etc.

- **Hacking** is the act of gaining unauthorized access to personal or organizational data. Hacking is not always a malicious activity, this act can be used identifying and then exploiting weaknesses in a computer system or network, *the notion of the “hack” is a “neat” technological trick and the idea of playfulness*, but the term has mostly negative connotations due to its association with cybercrime.

- **Cracking** is a technique that is used to gain unauthorized access into computer systems including software, or networks with malicious intent. Hence, Hackers referred to as white hat hackers and crackers, also referred to as black hat hackers. <sup>81</sup>

## 7.2 Types of Computer Crimes...

### 7.2.5 Denial of Service

A denial-of-service (DoS) is an attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to a network. Denial of service is typically accomplished by flooding the targeted machine or resource with superfluous requests in an attempt to overload systems and prevent some or all legitimate requests from being fulfilled.

There are two general methods of DoS attacks:

- **Crash attacks:** These attacks attempt to overwhelm a system with so much traffic that it crashes.
- **Flood attacks:** These attacks send a large number of requests to a system in an attempt to overload it.

### 7.2.6 Computer Invasion of Privacy

A crime that occurs when someone accesses or uses a computer or computer network with the intention of examining or disclose any employment, medical, salary, credit, or any other financial or personal data relating to any other person with knowledge that such examination without authority shall be guilty. Computer invasion of privacy can be made in a number of ways such as spyware, hacking, your ISP interfering with your connection etc.

## 7.2 Types of Computer Crimes...

### 7.2.7 Harmful Content Crime

Harmful Content Crime is a crime that involves the creation, distribution, or possession of harmful content using digital technology that causes others to distress or harm, such as child pornography, religious beliefs, views on racial matters etc.

### 7.2.8 Online Pornography

**Online pornography** or Internet pornography is any pornography that is accessible over the Internet, primarily via websites, peer-to-peer file sharing, or Usenet newsgroups. The availability of widespread public access to the World Wide Web in 1991 led to the growth of Internet pornography. The Internet is an international network and there are currently no international laws regulating pornography; each country deals with Internet pornography differently. However, all are agreed that pornography becomes a crime when it is considered obscene. Obscene material is so offensive it violates all standards of morality or civility. Online pornography available in different formats such as image files, video files etc.

## 7.2 Types of Computer Crimes...

### 7.2.9 Online Harassment

Online harassment can be defined as the use of information and communication technologies by an individual or group to cause harm, threats, embarrassment or humiliation to others.

Online harassment can have a devastating impact on victims, both emotionally and physically. It can lead to feelings of fear, anxiety, depression, and isolation. In some cases, it can even lead to suicide.

There are different types of online harassment such as threatening messages, humiliating or sexual content, disclose personal information etc.

### 7.2.10 Cyber Stalking and Online Scams

**Cyberstalking** is the use of the Internet or other electronic means such as email, social media, text messages etc. to stalk or harass an individual, group, or organization.

**Online Scam** is the use of information and communication technologies to steal personal information or other valuables, typically for financial gain. There are many different types of online scams such as phishing scams, romance scams etc. <sup>84</sup>

## 7.2 Types of Computer Crimes...

### 7.2.11 Spams

**Spam** may be originated from sp(iced) + (h)am, is unsolicited electronic messages, typically sent by a large number of people to a large number of recipients in an attempt to force the message on people who would not otherwise choose to receive it, often used to promote products or services and can also be used to spread malware or phishing attacks.

### 7.2.12 Malicious Programs

Malicious programs, also known as Malware, or malicious software, is any program or file that is intentionally harmful to a computer, network or server. They can be used to steal data, damage files, or even take control of a computer. There are different types of malwares such as viruses, worms, Trojan horses etc.

#### Viruses

A computer virus is a type of computer program that, when executed, replicates itself by modifying other computer programs and inserting its own code into those programs to steal data, damage files, or even take control of a computer. C-Brain, Cascade, Bomb etc. are some examples of

## 7.2 Types of Computer Crimes...

### Malicious Programs...

**Worms:** A computer worm is a standalone malware computer program that replicates itself in order to spread to other computers. It often uses a computer network to spread itself, relying on security failures on the target computer to access it. It will use this machine as a host to scan and infect other computers.

The technical term “worm” comes from The Shockwave Rider, a 1975 science fiction novel written by John Brunner. Morris worm, Mydoom, Existential worms etc. are some examples of worms.

#### Trojan Horses

A Trojan horse is a program with a benign capability that conceals a sinister purpose. When the user executes a Trojan horse, the program performs the expected beneficial task. However, the program is also performing actions unknown to, and not in the best interests of, the user.

An example of a Trojan horse is Moxmex, first uncovered in 2008 in digital picture frames manufactured in China. It spread from digital picture frames to computer hard drives and other portable storage devices people attached to their PCs. The purpose of the Trojan horse appeared to be to steal passwords to online computer games. Notroj, and Run.me. are more examples of Trojan horses.

## 7.2 Types of Computer Crimes...

### 7.2.13 Cyber Terrorism

Cyberterrorism is the use of digital technology to intimidate or force, especially for political or ideological purposes. It is a type of cybercrime that involves the use of computers or computer networks to carry out violent acts or threaten, that result in the loss of life or significant bodily harm. Cyberterrorism can be used to disrupt or disable critical infrastructure, steal sensitive information, or cause widespread panic and fear such as:

- In 2017, the **WannaCry** ransomware attack infected over 200,000 computers in over 150 countries. The attack was particularly devastating in the United Kingdom, where it caused widespread disruption to hospitals, schools, and businesses.

## 7. Computer and Cyber Crimes...

### 7.3 Introduction to Digital forensics

Digital forensics (sometimes known as digital forensic science) is a branch of forensic science encompassing identifying, preserving, recovering, analyzing and presenting digital evidence. Digital evidence can be found on a variety of devices, including computers, smartphones, tablets etc. ie., all devices capable of storing digital data. It can be used in a variety of investigations, including criminal investigations, civil litigation, and internal investigations.

The goal of digital forensics is to collect and preserve evidence in a way that is admissible in court and can be used to solve crimes, recover lost data, and protect intellectual property.

## 8. Intellectual Property and Legal Issues

In most of the world there is a widely accepted notion that people have the right to own property either it is **physical assets** or **intellectual assets** and have different laws to protect these assets which necessitate as well as enforcement of legal issues.

**Legal issues**, concern questions of legality, justice, and compliance with the law. These issues are based on the existing legal framework in a particular jurisdiction and are usually governed by statutes, regulations, and judicial decisions such as intellectual property rights, employment discrimination, criminal law etc.

In Nepal, Government of Nepal also have different laws to resolve the legal issues arises during protection of intellectual property rights as well criminal activities such as Copyright act, Right to Information Act, Electronics Transaction Act etc.

## 8. Intellectual Property...

### 8.1 Intellectual properties

Intellectual property is any unique product or creation of the human intellect that has social as well as commercial value. He or she has a right to protect his or her invention for its usefulness with the help of different rights such as copyright, patent, trademark etc. Examples of intellectual property are books, songs, movies, paintings, inventions, chemical formulas, and computer programs as well as technologies etc.

#### 8.1.1 Copyright

Copyright is a right, enforceable by law, accorded to an inventor or creator of an expression. Such expressions may include creative works (literary, dramatic, musical, pictorial, graphic, artistic, and technological) together with audiovisual and architectural works and sound recordings. In general, every original work that has a tangible form and is fixed in a medium is protectable under the copyright law which defines certain rights to original works with the help of:

## 8.1 Intellectual properties...

### 8.1.1 Copyright...

1. The right to reproduce
2. The right to distribute
3. The right to display
4. The right to perform and use
5. The right to produce new on the basis of this

Nepal also have Copyright Act to protect creator's creation or work.

### 8.1.2 Patent

A patent is a way to provide an inventor with an exclusive right to a piece of intellectual property and is a public document that provides a detailed description of the invention. The owner of the patent can prevent others from making, using, or selling the invention for the lifetime of the patent, which is may vary on the basis of creation or work with the help of patent law. After the patent expires, anyone has the right to make use of its ideas.<sup>91</sup>

## 8.1 Intellectual properties...

### 8.1.3 Design

Design is the creation of a plan or convention for the construction of an object or a system (as in architectural blueprints, engineering drawings, business processes, circuit diagrams and sewing patterns). Design has different connotations in different fields In some cases the direct construction of an object (as in pottery, engineering, management, cowboy coding and graphic design) is also considered to be design and to protect this type of creation necessitates a design right.

### 8.1.4 Trademark

A trademark is a word, symbol, picture, sound, or color used to identify product or service. By a trademark, an owner, organization or company have the right to use it and the right to prevent others from using it. Through the use of a trademark, a company can establish a "brand name." Society benefits from branding because branding allows consumers to have more confidence in the quality of the products.

Nepal also have **Patent, Design and Trademark Act** to protect creator's

## 8.1 Intellectual properties...

### 8.1.5 Trade-secrets

A trade secret is a confidential piece of intellectual property that provides a company with a competitive advantage. Examples of trade secrets include formulas, processes, proprietary designs, strategic plans, customer lists, and other collections of information. The right of a company to protect its trade secrets is widely recognized by governments around the world. In order to maintain its rights to a trade secret, a company must take active measures to keep it from being discovered. For example, companies typically require employees with access to a trade secret to execute a confidentiality agreement.

**8.1.6 IPR in Nepal: "Copyright Act" and "Patent, Design and Trademark Act"**

**8.2 IT Related Laws in Nepal: IT Policy of Nepal, Right to Information Act, Electronics Transaction Act and Rules, Secure Password Practices Issued by GoN**