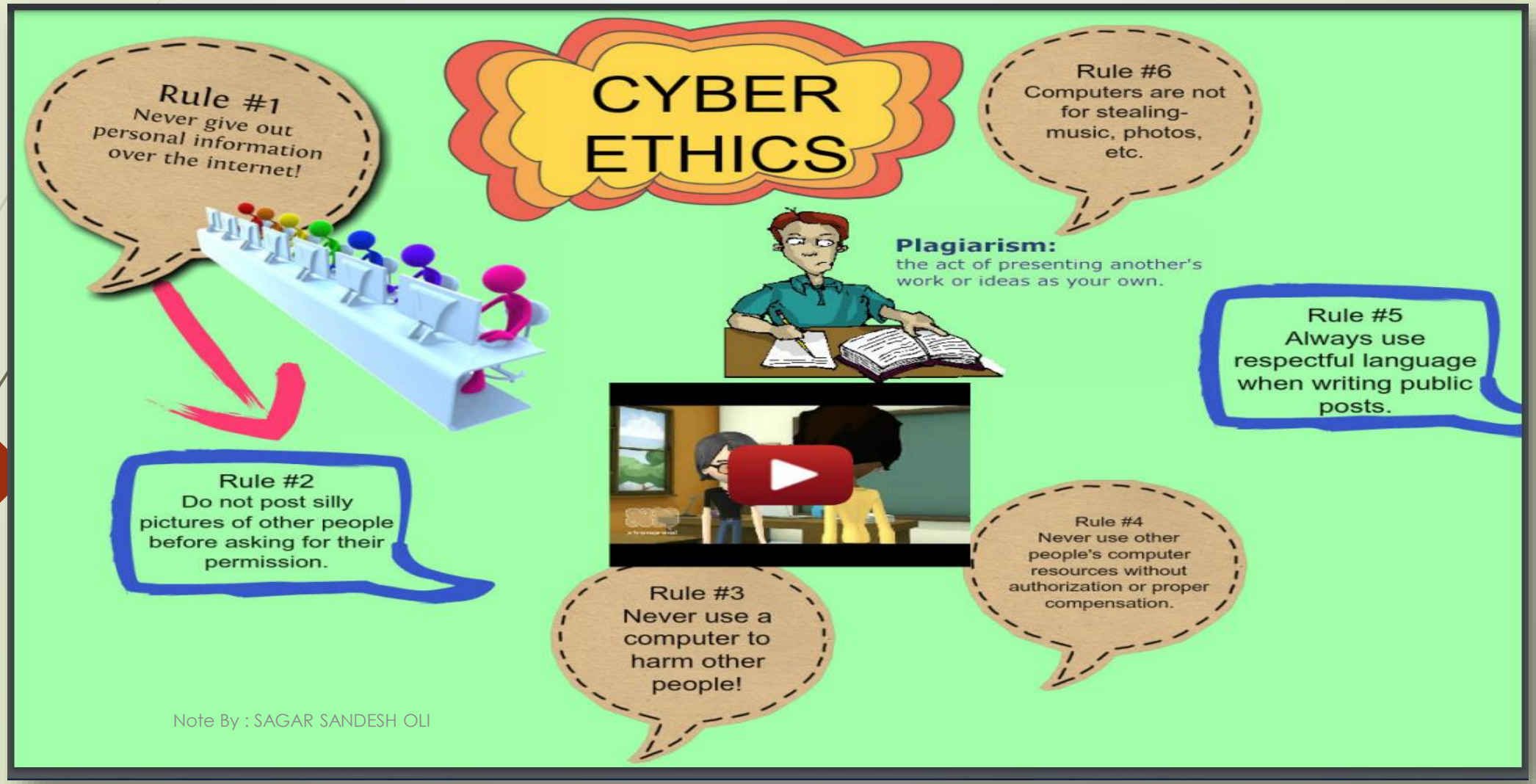
1.2 Ethical and Social Issues in ICT



2

2.1 Ethical and social Issues in ICT

a) What is ICT ?

ICT stands for Information and Communication Technologies . ICT is the type of technology which provides us a platform to create , store, access , transfer information through telecommunications. Computers , software , cell phones , internet , wireless network and other communication mediums.

- The rapid use of information and communication technology transformed the world into global village.
- Our society has became digital society it is because of advancement in ICT . The growing use of ICT has positive and negative impact on society. It has brought so many ethical and social issues for individuals and organizations.
- ICT Ethics are moral code of conduct or behavior to use ICT by individuals and society.
- Ethical and Social Issues are concern about the protection of personal privacy, intellectual property , user responsibility ,access and use of information , software license and piracy

Computer Ethics

Computer ethics is a set of moral principles or code of conducts that regulate the use of computers systematically without making harm to other users. It gives awareness to the user regarding the immoral behaviour and activities in the computing field.

Commandments of computer ethics

- Do not use a computer to harm other people.
- Do not use a computer to publish fake information.
- Do not search the file or record of other people.
- Do not destroy or delete the records of other people.
- Do not use a computer to steal someone's privacy.
- Do not interfere with other people's computer work.
- Do not snoop around in other people's files.
- Do not use or copy software for which you have not paid.
- Do not use other people's computer resources without authorization.

CYBERETHICS

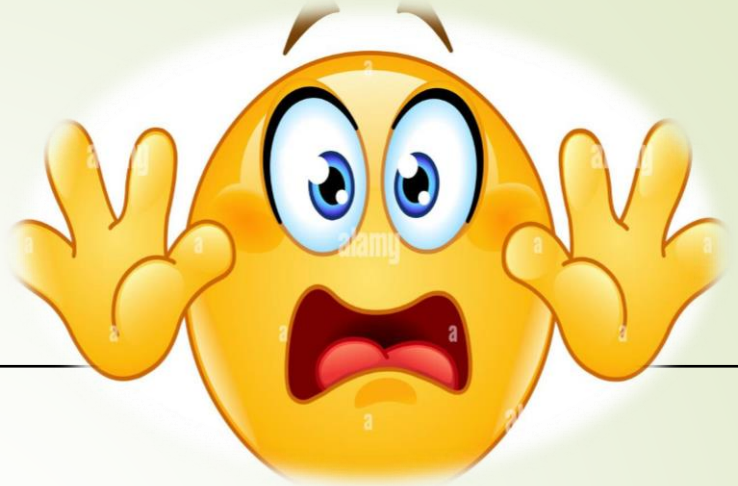
What are cyber ethics?

- Ethics are the rules you use in life to help you decide what is right and wrong.

- Cyber ethics is how you act when you are on the computer.

Rules of Cyber Ethics

1. Do not use rude or offensive language.
2. Don't be a bully on the Internet.
3. Do not call people names, lie about them, send embarrassing pictures of them, or do anything else to try to hurt them.
4. Do not copy information from the Internet and claim it as your own. That is called plagiarism.
5. Adhere to copyright restrictions when downloading material including software, games, movies, or music from the Internet.
6. Do not break into someone else's computer.
7. Do not use someone else's password.
8. Do not attempt to infect or in any way try to make someone else's computer unusable.



DO	DON'T
Do use the Internet to help you do your schoolwork.	Don't copy information from the Internet and call it your own.
Do use the Internet to learn about music, video and games.	Don't use the Internet to download or share copyrighted material
Do use the Internet to communicate with friends and family	Don't use the Internet to communicate with Strangers
	Don't give anyone personal information or Passwords
	Don't be rude or use bad language
	Don't pretend to be someone else

Digital Citizenship refers to the use of technology as a measure of behavior responsible for a digital society.

Digital Citizenship

Following are the elements of digital citizenship:

- Digital Access: The state of full electronic participation in society
- Digital Commerce: The act of promoting the purchase of goods through electronic means
- Digital Communication: Electronic exchange of information
- Digital literacy: Teaching and learning about teaching and technology
- Digital Security: Electronic precautions
- Digital Health: The solution to health problems using digital technology
- Digital Law: Act, rules and regulations required for performing electrical work

Digital Footprint

- A digital footprint is online identity of person that includes the activities of persons that exists on the internet.
- It includes the websites you visit , emails you send , and information you submit to online services .
- It is important to be aware of it because anything posted online is permanent and stays there forever regardless of being deleted.
- Digital footprints are of two types:

a) Active data trace b) Passive data trace

- Active data traces are the ones that the user leaves intentionally. Examples Facebook , Twitter and blog posts, social network connections, image and video uploads , emails , phone calls and chats.
- Passive data traces are the ones that an individual is left information by others and performing activities unknowingly. Example websites visiting, searching and online purchasing etc.

The following should be considered when managing Digital Footprint:

- Subscribed accounts and unused social media accounts which are no longer in use should be unsubscribed or deleted.
- Ensure the content posted protect your privacy.
- Not to forget that online posts are private.
- To note that parents, teachers and other people can view the content posted.
- Ensure the content posted does not damage yours or others reputation.

Cyberbullying

Cyberbullying is bullying that takes place over digital devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, Text, and apps, or online in social media, forums, or gaming where people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can nclude sharing personal or private information about someone else causing embarrassment or humiliation. Some cyberbullying crosses the line into unlawful or criminal behaviour.

Examples of cyberbullying:

- Sending rude emails, texts or instant messages online or on the phone
- Being excluded from online groups or forums
- Offensive chat on online gaming
- Posting hurtful things about someone on social media
- Spreading rumours or gossip about someone online
- Making fun of someone in an online chat that includes multiple people
- Attacking or killing an avatar or character in an online game, constantly and on purpose
- Pretending to be another person by creating a fake online profile
- Threatening or intimidating someone online or in a text message
- Taking an embarrassing photo or video and sharing it without permission

Cyber Law

Cyber law describes the legal issues related to using of inter-networked information technology. Cyber law is a term that encapsulates the legal issues related to the use of communicative, transactional, and distributive aspects of networked information devices and technologies.

(Cyberspace is the virtual environment created by the Internet and devices and services related to the Internet.)

ICT Policy 2072

- Enhancement of overall national ICT readiness with the objective of being at least in the top second quartile of the international ICT development index and e-Government rankings by 2020
- 75 % of the population to have digital literacy skills by the end of 2020
- Universal broadband access to all people on an equitable basis to be in place. By 2020, 90 percent of the population to have access to broadband services
- The role and significance of ICT industries and services (including telecom services) to increase in the Nepali economy with ICT value added (including digital content and service industry) accounting for at least 7.5% of GDP by 2020
- Apex level institutional arrangement to be restructured to effectively drive ICT agenda in the country in the light of emerging technologies and application trends shaping the sector
- By 2020, entire population of Nepal to have access to Internet
- 80% of all citizens facing government services to be offered online by 2020

Electronic Transaction Act (ETA)

- Transactions of electronics records data by using any types of electronics means.
- Contains electric records and valid digital medium.
- The exchange of all types of records which are in the form of electronic.

- ETA deals with issues related to cybercrime and also help in making and implementing laws over cybercrime.
- It has made different requirements so that if anyone found having cybercrime , he/she will be punished according to the scene of the crime.
- He/she can be jailed for minimum from 6 months to a maximum of 3 years and has to pay penalty according to the offense.
- Maintaining privacy in the cyberspace , creating strong passwords , updating the security software, updating password are some of the techniques to keep secure him/her.

Opportunities and Threats in Social Media

i. Brand Development
ii. Target Audience
iii. Customer Interaction
iv. Attracting Customer
v. Research

i. Social Engineering
ii. Targeted Phishing Attacks
iii. Fake Accounts
iv. Social Media used for spreading spam and malware