Computer Ethics

Definition of Computer Ethics

Ethics is a set of moral principles that govern the behavior of a group or individual. Computer ethics can be defined as the set of moral principles that regulate the use of computers.

Responsible use of Computer and Internet

The following are the basic security measures taken to prevent damage to computer system.

1. There must be adequate ventilation.
2. Adequate space must be allowed between each system unit.
3. Avoid dust by using cover.
4. Avoid moisture.
5. Provision of air conditioners and fans or other cooling machines.
6. Provision of UPS (Uninterruptible Power Supply) and other electrical appliances to avoid loss of information and electrical damage to the system.
7. Adequate care must be taken to storage devices like diskettes, flash drive, CD/DVD writer drive, etc.
8. Disallow an unauthorized user from having access to your computer.
9. Ensure maximum security to files and information on the computer.
10. Provide computer with anti-virus program to avoid viruses.
11. Avoiding food particles dropping into the system.
12. Unplug the system when not in use for long.

13. Check your email regularly.
14. Give prompt and polite response to mails.

Reasons for Taking Care of the Computer

a. To avoid damage to files
b. To protect the system
c. To prolong the life of the system
d. To make the user comfortable for maximum efficiency.

Areas of Misusing the Computer

The following are areas in which computer can be misused.

1. Invasion of privacy (hacking): through the internet, a lot of information can be passed to several places and among people. To this end, the privacy of information cannot be guaranteed; hence someone can have access to another person's information. People who gain unauthorized access to a computer system or data belonging to somebody else are called a hacker. They invade computer database to steal the identities of other people by obtaining private information about them.

2. Computer virus: This can affect the computer through the internet where unsolicited information is sent to destroy files in other computers. Computer virus can also occur where diskette, CDs, DVDs, flash drives that are have been corrupted are used in another computer. It is therefore necessary to that anti-virus programs are installed in our computers to detect and clean any virus that may want to attack our computers.

3. Fraud: Through the internet and computer networks a lot of deception and scam can be perpetrated by dubious people

4. Stealing: people can steal very important documents, information and money through the misuse of computer and the internet.

5. Pornography: Children and adults misuse the computer by watching pornographic films and pictures on the internet. These are pictures of nude people and obscene sexual acts on the internet.

6. Cyber war: this is the use of computer and the internet in conducting warfare in cyberspace. The type of attacks include web vandalism, propaganda, where political messages can be spread through or to anyone with access to the internet, equipment destruction, where military activities that use computers and satellites for coordination are at risk and their communications and orders intercepted or replaced thereby putting soldier at risk.

7. Software piracy: This is the situation where programs written by people are used without their permission.

8. Plagiarism: This is the situation where the original works of people especially books and other works are copied verbatim (word for word). Without due acknowledgement of the owner. All this can happen on the internet.