



## Topic: 1.5 Ethics

Ethics can be explained as "moral principles that governs one or many people's behaviors." Ethical behavior is not necessarily related to the law. For example, just because something is not against the law doesn't mean it is okay to do it.

It's an area of study that deals with ideas about what is good and bad behavior, a branch of philosophy dealing with what is morally right or wrong. Further we can put a word that Ethics is a belief that something is very important.

The Theme of ethics comprises systematizing, defending, and recommending concepts of right and wrong behavior. Philosophers today usually divide ethical theories into three general subject areas:

- 1) Met ethics
- 2) Normative ethics
- 3) Applied ethics

**Zak** Met ethics investigates where our ethical principles come from, and what they mean. Are they merely social inventions? Do they involve more than expressions of our individual emotions? Met ethical answers to these questions focus on the issues of universal truths, the will of God, the role of reason in ethical judgments, and the meaning of ethical terms themselves.

**Zak** Normative ethics takes on a more practical task, which is to arrive at moral standards that regulate right and wrong conduct. This may involve articulating the good habits that we should acquire, the duties that we should follow, or the consequences of our behavior on others.

**Zak** Finally, applied ethics involves examining specific controversial issues, such as abortion, infanticide, animal rights, environmental concerns, homosexuality, capital punishment, or nuclear war.





## Topic: 1.5 Ethics

### ETHICS OF COMPUTER

Computer ethics is concerned with the procedures, values and practices that govern the process of consuming computing technology and its respective disciplines without harming or violating the moral values and beliefs of any personal, organization or entity.

Computer ethics is a perception in ethics that addresses the ethical issues and constraints that crop up from the use of computers, and how they can be mitigated or barred

Computer ethics can be understood as that branch of applied ethics which studies and analyzes social and ethical impact of information technology.

### Ten Commandments dealing with computer ethics to steer to a responsible computer use

- Zak Thou shall not use a computer to harm other people.
- Zak Thou shall not interfere with other people's computer work.
- Zak Thou shall not snoop around in other people's computer files.
- Zak Thou shall not use a computer to steal.
- Zak Thou shall not use a computer to bear false witness (aka Lie).
- Zak Thou shall not copy or use proprietary software for which you have not paid.
- Zak Thou shall not use other people's computer resources without authorization or proper compensation.
- Zak Thou shall not appropriate other people's intellectual output.
- Zak Thou shall think about the social consequences of the program you are writing or the system you are designing.
- Zak Thou shall always use a computer in ways that ensure consideration and respect for your fellow humans.

### Copyright and plagiarism

Copyright laws (title 17, U. S. Code) provide protection to the authors of "original works of authorship," including literary, dramatic, musical, artistic, and certain other intellectual works. This protection is available to both published and unpublished works. For complete copyright information, see the United States Copyright Office's web page.

Under copyright law, if you don't own the copyright to a work, you cannot do the following without permission from the copyright holder:

- Zak Reproduce copies of the work
- Zak Create derivative works based on the work
- Zak Distribute copies of the work
- Zak Perform the work publicly
- Zak Display the work publicly





## Topic: 1.5 Ethics

However, under certain circumstances, using parts of copyrighted works is considered "fair use," and is allowable under the law. Courts consider these four factors in determining whether or not a particular use is fair:

- The purpose and character of the use, including whether such use is of commercial nature or is for nonprofit educational purposes;
- The nature of the copyrighted work;
- Amount and substantiality of the portion used in relation to the copyrighted work as a whole and the effect of the use upon the potential market for or value of the copyrighted work.

### ESSENTIAL COMPONENTS OF A PERSONAL CODE OF COMPUTER ETHICS

- Honesty
- Respect
- Confidentiality
- Professionalism
- Responsibility
- Communication
- Obeying the law

### Plagiarism

Using someone else's thoughts or ideas as your own without properly giving credit is plagiarism. It is your responsibility to understand what plagiarism is and know how to avoid it.

Read the following very carefully: **Plagiarism is a serious crime!** Now, repeat it to yourself again. Why is this so important? Plagiarism is something that students easily fall into, whether they mean to or not. When you write a report and copy and paste from the Internet, you are committing plagiarism. So, what exactly is plagiarism and how can you avoid it?

When someone publishes work, including books, music, photographs, movies, software, paintings, poetry, articles, etc., they are granted copyright. Copyright is a set of rights given to the creator of the work allowing them the sole right to copy and distribute the work. This means that only they can copy, use, or sell the work. For example, a common myth is that when we buy a CD, we own the music. That is not true! We have purchased the right to enjoy the music, but it is not ours to copy and then give to a friend. That is a violation of copyright. The same goes for that example of writing a report. If you copy and paste or write word for word someone else's work, you are violating copyright laws.

Let's get back to plagiarism. In a nutshell, plagiarism is taking credit for work that someone else did. The Internet makes plagiarism very easy to do. However, the Internet also makes it very easy for a teacher to check your work for plagiarism. Be smart and avoid plagiarism at all costs.





## Topic: 1.5 Ethics

### Copyright V/s. Plagiarism

Copyright	Plagiarism
One who violets copyright breaks laws that protect the right of the creator of an original work.	One who plagiarizes breaks a moral code by claiming credit for the work of someone else.
Violation of copyright law may results in fines, imprisonment or both.	Plagiarism may result in academic dismissal or loss of job.

### Piracy and Illicit Downloading

Another legal issue in computing is software piracy and illegal downloading. Piracy is the illegal use and/or copying of software. This includes not only software used on the computer, but video games, DVDs, CDs, and MP3 files. Notice that the terms "use" AND "copying" were used. Even if you aren't the one who makes the copy, you are still breaking the law by using a "bootlegged" copy.

Think about it this way. Let's say that your friend just illegally downloaded the hottest new movie and makes a copy for a few of his friends. You say to yourself, "no big deal...the actors in these movies are filthy rich anyway". However, this is wrong way of thinking. It isn't really the actors that you hurt when you "steal" this way. Think about the people who produce the movie. Think about the people who run the cameras. Think about the people who keep the studio clean. When you steal music, movies, and software, you affect a lot of different people.

### What is FREE SOFTWARE?

"Free software" means software that respects users' freedom and community. Roughly, it means that **the users have the freedom to run, copy, distribute, study, change and improve the software**. Thus, "free software" is a matter of liberty, not price. To understand the concept, you should think of "free" as in "free speech," not as in "free beer".

We campaign for these freedoms because everyone deserves them. With these freedoms, the users (both individually and collectively) control the program and what it does for them. When users don't control the program, we call it a "non-free" or "proprietary" program. The non-free program controls the users, and the developer controls the program; this makes the program an instrument of unjust power

A program is free software if the program's users have the four essential freedoms:

-  The freedoms to run the program as you wish for any purpose (freedom 0).
-  The freedom to study how the program works and change it so it does your computing as per your requirements (freedom 1). (*Access to the source code is a precondition for this.*)





## Topic: 1.5 Ethics

-  The freedom to redistribute copies so you can help your neighbor or your peers (freedom 2).
-  The freedom to distribute copies of your modified versions to others (freedom 3). By doing this you can give the whole community a chance to benefit from your changes.  
(Access to the source code is a precondition for this.)

A program is free software if it gives users adequately all of these freedoms. Otherwise, it is not free. While we can distinguish various non-free distribution schemes in terms of how far they fall short of being free, we consider them all equally unethical.

*The following clarifies certain points about what makes specific freedoms adequate or not.*

Freedom to distribute (freedoms 2 and 3) means you are free to redistribute copies, either with or without modifications, either gratis or charging a fee for distribution, to anyone anywhere. Being free to do these things means (among other things) that you do not have to ask or pay for permission to do so.

You should also have the freedom to make modifications and use them privately in your own work or play, without even mentioning that they exist. If you do publish your changes, you should not be required to notify anyone in particular, or in any particular way.

The freedom to run the program means the freedom for any kind of person or organization to use it on any kind of computer system, for any kind of overall job and purpose, without being required to communicate about it with the developer or any other specific entity. In this freedom, it is the *user's* purpose that matters, not the *developer's* purpose; you as a user are free to run the program for your purposes, and if you distribute it to someone else, then he/she is then free to run it for his/her purposes, but you are not entitled to impose your purposes on her.

The freedom to run the program as you wish means that you are not forbidden or stopped from doing so. It has nothing to do with what functionality the program has, or whether it is useful for what you want to do.

The freedom to redistribute copies must include binary or executable forms of the program, as well as source code, for both modified and unmodified versions. (Distributing programs in executable form is necessary for conveniently running on operating systems.) It is OK if there is no way to produce a binary or executable form for a certain program (since some languages don't support that feature), but you must have the freedom to redistribute such forms should you find or develop a way to make them.

In order for freedoms 1 and 3 (the freedom to make changes and the freedom to publish the changed versions) to be meaningful, you must have access to the source code of the program. Therefore, accessibility of source code is a necessary condition for free software. Ambiguous "source code" is not real source code and does not count as source code.





## Topic: 1.5 Ethics

Freedom 1 includes the freedom to use your changed version in place of the original. If the program is delivered in a product designed to run someone else's modified versions but refuse to run yours – a practice known as “tivoization” or “lockdown”, or (in its practitioners' perverse terminology) as “secure boot” – freedom 1 becomes a theoretical fiction rather than a practical freedom. This is not sufficient. In other words, these binaries are not free software even if the source code they are compiled from is free.

One important way to modify a program is by merging with available free subroutines and modules. If the program's license says that you cannot merge in a suitably licensed existing module – for instance, if it requires you to be the copyright holder of any code you add – then the license is too restrictive to qualify as “free”.

Freedom 3 includes the freedom to release your modified versions as free software. A free license may also permit other ways of releasing them; in other words, it does not have to be a copy left license. However, a license that requires modified versions to be non-free does not qualify as a free license.

In order for these freedoms to be real, they must be permanent and irrevocable as long as you do nothing wrong; if the developer of the software has the power to revoke the license, or retroactively add restrictions to its terms, without your wrong doings, then the software is not free.

However, certain kinds of rules about the manner of distributing free software are acceptable, when they don't conflict with the central freedoms. For example, copy left (very simply stated) is the rule that when redistributing the program, you cannot add restrictions to deny other people the central freedoms. This rule does not conflict with the central freedoms; rather it protects them.

### Freeware Software:

Freeware is copyrighted software that is licensed to be copied and distributed without charges.

Freeware is free because the license says it is, but it's still under the owner's control.

Example:

 Netscape

 Internet Explorer





## Topic: 1.5 Ethics

### Shareware Software:

The software is licensed for copying and sharing for a trial period, but payment must be made to the owner for permanent use.

### ETHICAL ISSUES OF ELECTRONIC COMMUNICATION

There is little doubt that electronic communications, and in particular e-mail, have introduced a paradigm shift in management, organizational and working methods, as well as in business performance, as they have in the economy in general. While ICTs have dramatically improved business-to-business or business-to-consumers communications, they have also significantly impacted our day-to-day personal and professional lives. In particular, many organizations and their employees seem to have been overwhelmed by a number of issues arising from the usage of electronic communications in the professional environment.

### HACKING

Hacking has always been a controversial issue. Whether people see it as a vigilante attempt at justice, an attempt to keep authority in check or simply a way to cause mischief and potentially serious harm, it has always had its pros and cons.

Hacking has been around for longer than the word itself. The original use of the word "hack" came from the Massachusetts Institute of Technology, and it described a creative or witty way of doing almost anything. This soon grew to include creative practical jokes that involved some degree of stealth whether literal or simply in its implementation. Soon the word began to imply some degree of harm done to the "victim." Many who call themselves hackers insist that if their actions are inflicting harm, then it is not hacking, but "cracking."

The term "hacking" was originally used to describe ways to create, alter or improve software and hardware. - A "hacker" is an extremely proficient programmer that could do tasks in 5 lines of code what others would take several modules.

### CRACKING

"Cracking" is the illegal version of hacking, where existing software is reverse-engineered to remove restrictions like trial periods.

These days, most people don't know the difference anymore, as the term "hacking" has also been used to describe the action of "breaking into someone's system"





## Topic: 1.5 Ethics

### PRODUCTION OF MALWARE

Malware (short for "malicious software") is any software designed to harm your computer, such as viruses, worms, Trojan horses, and root kits.

- Zak** A **computer virus** is a program that attaches itself to an application or "host file" and then spreads by making copies of it. Some type of human action (e.g. opening an attachment) is always required for a virus to take effect. Once a virus gets onto your computer it might modify, delete, or steal your files, make your system crash, or take over your machine.
- Zak** A **computer worm** is like a virus, but it infects other computers all by itself, without human action and without a host file. It usually infects other computers by sending emails to all the names in your email address book.
- Zak** A **Trojan horse** is a program that tricks you into running it by appearing useful or harmless. However, once it is run, it damages your computer, usually by providing "back door" access to the computer. This allows hackers to control or use your computer, destroy or steal files, install viruses or spyware, or run arbitrary programs.
- Zak** A **root kit** is a program that allows an intruder to gain access to your system without your knowledge by hiding what it is doing on the system. The intruder can then install difficult-to-detect back doors into your system to seize control.

### Protective Measures

#### Practices

- Zak** **Only perform file transfers from trusted sources:** This reduces your risk of downloading files infected with malware and introduces accountability, so that you have a better chance of getting a response if you do have a problem.
- Zak** **Scan all files that you receive through file transfer:** It is a good idea to scan the files that you receive from P2P networks with your anti-virus software to detect malware. This may slow down the transfer, but it will help keep your computer safe.
- Zak** **Check a corporate wireless network's security level before connecting:** Many corporate networks allow users to connect their wireless devices to the network. However, not all of these networks are secured. In fact, it is quite easy for a user to connect his/her wireless device to a corporate network without getting permission first. When this happens, the user may intentionally or unintentionally transfer viruses onto the company network, putting everybody on the network at risk. You should make sure your corporate network is secure before connecting your own device. If users can connect to your company's network without getting permission or a password, it's probably not a good idea to connect to that network at all.





### Topic: 1.5 Ethics

 **Make sure the public network you connect to is secure:** Many public networks are not secure and do not even require you to identify yourself with a password. Not only do you run the risk of being infected by malware from other users on such a network, you may unintentionally transmit malware to them as well. Make sure you only connect to secured networks that ask users for a password.

Unfortunately, wireless cards and operating systems are set up to automatically connect to any network in range. Disabling or modifying this setting requires a thorough understanding of your operating system, so you should generally leave this setting alone. Your best option is to check the network every time you connect and manually disconnect if the network is not secure.

A full field of malware creation tools has enabled attackers to transition from manually creating single-use and easily defeated malware to developing an automated production line to develop an "army of armored malware" to carry out attack campaigns and hence bring harm to you and your PC.

