# Code of Ethics and Professional Conduct

The Code is designed to inspire and guide the ethical conduct of all computing professionals, including current and aspiring practitioners, instructors, students, influencers, and anyone who uses computing technology in an impactful way.

## **1. GENERAL ETHICAL PRINCIPLES.**

A computing professional should...

### 1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.

### 1.2 Avoid harm.

### 1.3 Be honest and trustworthy.

### 1.4 Be fair and take action not to discriminate.

### 1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.

### 1.6 Respect privacy.

## 2. PROFESSIONAL RESPONSIBILITIES.

A computing professional should…

2.1 Strive to achieve high quality in both the processes and products of professional work.

2.2 Maintain high standards of professional competence, conduct, and ethical practice.

2.3 Know and respect existing rules pertaining to professional work.

2.4 Accept and provide appropriate professional review.

### 2.5 Perform work only in areas of competence.

### 2.6 Foster public awareness and understanding of computing, related technologies, and their consequences.

### 2.7 Access computing and communication resources only when authorized or when compelled by the public good.

### 2.8 Design and implement systems that are robustly and usably secure.

## 3. PROFESSIONAL LEADERSHIP PRINCIPLES.

### 3.1 Ensure that the public good is the central concern during all professional computing work.

### 3.2 Manage personnel and resources to enhance the quality of working life.

### 3.4 Create opportunities for members of the organization or group to grow as professionals.

## 4. COMPLIANCE WITH THE CODE.

A computing professional should...

### 4.1 Uphold, promote, and respect the principles of the Code.

**Programming Code Of Ethics**

Key points of proper conduct for Computer Programmers-  
  
A programmer must...

* never create or distribute malware.
* never write code that is intentionally difficult to follow.
* never write documentation that is intentionally confusing or inaccurate.
* never reuse copyrighted code unless the proper license is purchased or permission is obtained.
* acknowledge (verbally and in source code comments) the work of other programmers on which the code is based, even if substantial changes are made.
* never intentionally introduce bugs with the intent of later claiming credit for fixing the bugs, or to stimulate the uptake of later versions.
* never write code that intentionally breaks another programmer's code for the purpose of elevating one's status.
* never hide known obstacles to a project's completion during any phase of development, especially the design phase.
* report any illegal activities of the employer.
* never falsely deny the presence of bugs.
* never reveal the secret corporate knowledge of an employer.
* never accept compensation from multiple parties for the same work unless permission is given.
* never conceal from the employer their financial interest in development resources.
* never maliciously injure the reputation of an employer or members of the development team.
* never take credit for another's work.
* never steal software, especially development tools.
* never install third-party applications without the user's permission.

**IT Policy**

Companies provides and maintains technological products, services and facilities like Personal Computers (PCs), peripheral equipment, servers, telephones, Internet and application software to its employees for official use. The Information Technology (IT) Policy of the organization defines rules, regulations and guidelines for proper usage and maintenance of these technological assets to ensure their ethical and acceptable use and assure health, safety and security of data, products, facilities as well as the people using them. It also provides guidelines for issues like purchase, compliance, IT support and grievance redressal of the employees pertaining to technological assets and services used for office work.

* Acceptable Use Policy
* Security awareness
* DR/BCP ([Disaster Recovery](http://www.csoonline.com/article/2858340/disaster-recovery/why-disaster-recovery-planning-can-save-lives.html), Business Continuity plan)
* Change management
* Equipment Usage policy
* PC standards
* The Internet Usage Policy
* Information security Policy
* Email and chat Policy
* The Software Usage Policy