



ORACLE

Academy



Computer Social, Ethical, and Risk Impacts



ORACLE
Academy

¹ [ACM Code of Ethics and Professional Conduct](#)

Objectives

- This lesson covers the following objectives:
 - Identify the ethical and social implications of computing systems
 - Identify the responsibility to maximize system reliability
 - Compare the benefits and harmful impacts of computers
 - Identify risks to privacy from collecting and storing personal data
 - Identify the responsibility to safeguard data privacy



1 - General Ethical Principles

- 1.1: Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing
 - Promote fundamental human rights
 - Protect everyone's right to autonomy
 - Minimize negative consequences including
 - threats to health, safety, personal security, and privacy
 - Respect diversity
 - Contribute to society by engaging in pro bono or volunteer work that benefits the public good
 - Promote a safe social environment and environmental sustainability



1 - General Ethical Principles

1.2: Avoid harm (negative consequences)



- Examples of harm:
 - unjustified physical or mental injury, destruction or disclosure of information, or damage to property, reputation, and the environment
- Well-intended actions, including those that accomplish assigned duties, may lead to harm
 - When that harm is unintended, those responsible are obliged to undo the harm as much as possible
- Follow best practices unless there is a compelling ethical reason to do otherwise
- Analyze the consequences of data aggregation and emergent properties of systems
- Report risks that might result in harm

1 - General Ethical Principles

1.3: Be honest and trustworthy

- Be transparent and provide full disclosure of system capabilities, limitations, and problems
- Be honest about your limitations in your competence to complete a task
- Honor commitments
- Avoid conflicts of interest
- Do not speak on behalf of an organization unless authorized



1 - General Ethical Principles

1.4: Be fair and take action not to discriminate

- Maintain fair participation (inclusive and accessible) of all people, including those of underrepresented groups
- Discrimination limits fair access to virtual and physical spaces
- Discrimination includes prejudices based on:
 - age, color, disability, ethnicity, family status, gender identity, labor union membership, military status, nationality, race, religion or belief, sex, sexual orientation
- Avoid creating systems or technologies that may cause new, or enhance existing inequities



1 - General Ethical Principles

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

- Credit the creators of ideas, inventions, work, and artifacts
- Respect copyrights, patents, trade secrets, license agreements, and other methods of protecting authors' works
- Some exceptions to a creator's control of a work are necessary for the public good
 - These efforts include free and open-source software and work put into the public domain



1 - General Ethical Principles



1.6: Respect privacy

- Understand the various definitions and forms of privacy, and the rights and responsibilities associated with the collection and use of personal information
- Use personal information for legitimate ends and without violating the rights of individuals and groups
- Establish procedures that allow individuals to understand what data is being collected and how it is being used
- Use informed consent for automatic data collection, and to review, obtain, correct inaccuracies in and delete their personal data
- Collect only personal information that is necessary
- Take special care for privacy when merging data collections

1 - General Ethical Principles



1.7: Honor confidentiality

- Protect confidential information, such as, trade secrets, client data, nonpublic business strategies, financial information, research data, pre-publication scholarly article, and patent applications
- Exceptions to divulgence of this information is to not violate law, or organizational regulations
- Divulgence should be made to appropriate authorities

2 - Professional Responsibilities

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

- Insist on and support high-quality work from yourself and colleagues
- Dignity of employers, employees, colleagues, clients, users, and anyone else affected by the work is to be respected
- Be cognizant of (and do not neglect) any serious negative consequences affecting any stakeholder that results from poor quality work



2 - Professional Responsibilities

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

- Professional competence
 - Starts with technical knowledge and awareness of the social context in which your work may be deployed
 - Requires skill in communication, reflective analysis, and recognizing and navigating ethical challenges
- Upgrading skills should be ongoing, and might include independent study, conferences, seminars, and formal education



2 - Professional Responsibilities

2.3: Know and respect existing rules pertaining to professional work

- Local, regional, national, and international laws and regulations, as well as any policies and procedures of the organization to which you belong are considered rules
- Rules that are considered unethical should be challenged
- Use existing channels to challenge rules
- An employee who Decides to violate a rule because it is unethical should consider potential consequences and accept responsibility



2 - Professional Responsibilities

2.4: Accept and provide appropriate professional review

- High-quality professional work in computing depends on professional review at all stages
- Seek and utilize peer and stakeholder review
- Provide constructive, critical reviews of others' work



2 - Professional Responsibilities

2.5: Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks

- Computing professionals are in a position of trust, and therefore have a special responsibility to provide objective, credible evaluations and testimony to employers, employees, clients, users, and the public
- Be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives
- If future risks cannot be reliably predicted, the system should not be deployed

2 - Professional Responsibilities

2.6: Perform work only in areas of competence

- A computer professional is responsible for evaluating potential work assignments and if the work assignment is within the professional's areas of competence
- The professional should disclose lack of necessary expertise, allowing the client or employer to work with someone else, forgo the assignment, or allow additional time to acquire the necessary competencies



2 -Professional Responsibilities

2.7: Foster public awareness and understanding of computing, related technologies, and their consequences

- Computing professionals should share technical knowledge with the public, foster awareness of computing, and encourage understanding of computing
 - This includes impacts of computer systems, their limitations, their vulnerabilities and the opportunities that they present
- A Computer professional should respectfully address inaccurate or misleading information related to computing

2 -Professional Responsibilities

2.8: Access computing and communication resources only when authorized or when compelled by the public good

- Individuals and organizations have the right to restrict access to their systems and data so long as the restrictions are consistent with the code
- A system being publicly accessible is not sufficient grounds to imply authorization
- However, a computer professional may use unauthorized access to disrupt or inhibit malicious systems

2 -Professional Responsibilities

2.9: Design and implement systems that are robustly and usably secure

- Breaches of computer security cause harm
- Computing professionals should perform due diligence to ensure the system functions as intended, and take appropriate action to secure resources against accidental and intentional misuse, modification, and denial of service
- Computing professionals should also take steps to ensure parties affected by data breaches are notified in a timely and clear manner
- Security features should be designed to be as intuitive and easy to use as possible
- In cases where misuse or harm are predictable or unavoidable, the best option may be to not implement the system

3 - Professional Leadership Principles

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

- People – including users, customers, colleagues, and others affected indirectly or indirectly should always be the central concern in computing
- The public good should always be an explicit consideration when dealing with research, requirements analysis, design, implementation, testing, validation, deployment maintenance, retirement, and disposal



3 - Professional Leadership Principles

3.2 - Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group

- Technical organizations and groups affect broader society, and their leaders should accept the associated responsibilities
- Leaders should encourage full participation of computing professionals in meeting relevant social responsibilities and discourage tendencies to do otherwise



3 - Professional Leadership Principles

3.3 - Manage personnel and resources to enhance the quality of working life

- Leaders should ensure that they enhance, not degrade, the quality of working life
- Leaders should consider the personal and professional development, accessibility requirements, physical safety, psychological well-being, and human dignity of all workers using human-computer ergonomic standards



3 - Professional Leadership Principles

3.4 - Articulate, apply, and support policies and processes that reflect the principles of the Code

- Leaders should pursue clearly defined organizational policies that are consistent with the code and effectively communicate them to relevant stakeholders
- Leaders should encourage and reward compliance with those policies, and take appropriate action when policies are violated



3 - Professional Leadership Principles

3.5 - Create opportunities for members of the organization or group to grow as professionals

- Leaders should ensure that opportunities are available to computing professionals to help them improve their knowledge and skills in professionalism, in the practice of ethics, and in their technical specialties
- Computing professionals should be fully aware of the dangers of oversimplified approaches, the improbability of anticipating every possible operating condition, the inevitability of software errors, the interactions of systems and their contexts, and other issues related to the complexity of their profession

3 - Professional Leadership Principles

3.6 - Use care when modifying or retiring systems

- Interface changes, the removal of features, and even software updates have an impact on the productivity of users and the quality of their work
- Leaders should take care when changing or discontinuing support for system features on which people still depend
- Investigate alternatives to removing support for a legacy system, and if unacceptably risky, the developer should assist stakeholders' graceful migration from the system to an alternative
- Notify users of the risks of continued use of the unsupported system
- Help users understand that timely replacement of inappropriate or outdated features or systems may be needed

3 - Professional Leadership Principles

3.7 - Recognize and take special care of systems that become integrated into the infrastructure of society

- Even the simplest computer systems have the potential to impact all aspects of society when integrated with everyday activities such as commerce, travel, government, healthcare, and education
- It is an added responsibility to be good stewards of these systems
- Establish policies for fair system access
- Monitor the level of integration of these systems into society
- Continual monitoring of systems to include developing appropriate standards

Case Studies

- Choose one or more of the case studies from the Reference Materials for this lesson:
 1. Malware Disruption
 2. Linking Public Data Sets
 3. Medical Implant Risk Analysis
 4. Abusive Workplace Behavior
 5. Malicious Input to Content Filters
- You may discuss the case study in class, or assign with instructions to comment and summarize



Summary

- In this lesson, you should have learned how to:
 - Identify the ethical and social implications of computing systems
 - Identify the responsibility to maximize system reliability
 - Compare the benefits and harmful impacts of computers
 - Identify risks to privacy from collecting and storing personal data
 - Identify the responsibility to safeguard data privacy



ORACLE

Academy