ACM CODE OF ETHICS AND PROFESSIONAL CONDUCT

GUIDING PRINCIPLES FOR COMPUTING PROFESSIONALS

PRESENTED BY: DR. RAZIB HAYAT KHAN

INTRODUCTION

- What is the ACM?
- Importance of Ethics in Computing
- Purpose of the ACM Code of Ethics

STRUCTURE OF THE CODE

- General Ethical Principles
- Professional Responsibilities
- Leadership Responsibilities
- Compliance with the Code

PRINCIPLE 1.1 – CONTRIBUTE TO SOCIETY AND TO HUMAN WELL-BEING

- Promote human rights and environmental sustainability
- Minimize negative consequences like privacy violations
- Engage in pro bono or volunteer work

PRINCIPLE 1.2 – AVOID HARM

- Identify and mitigate harms
- Report risks responsibly
- Use best practices and ethical justification for any intentional harm

PRINCIPLE 1.3 – BE HONEST AND TRUSTWORTHY

- Provide full disclosure of system capabilities and limitations
- Avoid deception, honor commitments
- Be transparent about qualifications

PRINCIPLE 1.4 – BE FAIR AND TAKE ACTION NOT TO DISCRIMINATE

- Avoid prejudicial discrimination
- Design inclusive and accessible systems
- Promote fairness in decision-making

PRINCIPLE 1.5 – RESPECT INTELLECTUAL PROPERTY

- Credit original creators
- Respect legal protections like copyrights and patents
- Support open-source and public domain contributions

PRINCIPLE 1.6 – RESPECT PRIVACY

- Use data only for legitimate ends
- Ensure transparency and informed consent
- Minimize data collection and retention

PRINCIPLE 1.7 – HONOR CONFIDENTIALITY

- Protect sensitive information
- Disclose only to appropriate authorities when necessary

PRINCIPLE 2.1 – HIGH QUALITY IN WORK

- Insist on high standards in processes and products
- Respect dignity and transparent communication
- Avoid inducements to compromise quality

PRINCIPLE 2.2 – MAINTAIN PROFESSIONAL COMPETENCE

- Stay current with skills and knowledge
- Engage in continuous learning and development
- Encourage professional growth in teams

PRINCIPLE 2.3 – KNOW AND RESPECT LAWS

- Follow legal and organizational policies
- Challenge unethical rules responsibly
- Accept consequences of ethical decisions

PRINCIPLE 2.4 – ACCEPT AND PROVIDE REVIEW

- Participate in peer and stakeholder review
- Provide constructive feedback
- Improve quality through collaboration

PRINCIPLE 2.5 – EVALUATE SYSTEMS AND RISKS

- Analyze potential consequences
- Report major risks
- Avoid deployment of unsafe systems

PRINCIPLE 2.6 – WORK WITHIN COMPETENCE

- Evaluate assignments for feasibility
- Disclose limits of expertise
- Acquire skills or defer tasks responsibly

PRINCIPLE 2.7 – FOSTER PUBLIC UNDERSTANDING

- Educate others about computing impacts
- Address misinformation respectfully
- Promote responsible use of technology

PRINCIPLE 2.8 – ACCESS RESOURCES ETHICALLY

- Avoid unauthorized access
- Act only under public good with care
- Mitigate harm in exceptional cases

PRINCIPLE 2.9 – BUILD SECURE SYSTEMS

- Design for robust and usable security
- Monitor and patch vulnerabilities
- Inform stakeholders about breaches

LEADERSHIP RESPONSIBILITY – PUBLIC GOOD AS CENTRAL CONCERN

- Consider impact on all stakeholders
- Apply ethics in every project phase
- Use ethical methodologies and design

LEADERSHIP – ENCOURAGE ETHICAL CONDUCT

- Foster social responsibility
- Promote full participation
- Discourage unethical behavior

LEADERSHIP – ENHANCE QUALITY OF WORK LIFE

- Support well-being and safety
- Respect ergonomic and accessibility needs
- Provide growth opportunities

LEADERSHIP – ETHICAL POLICY AND PROCESSES

- Define and communicate ethical policies
- Reward compliance, address violations
- Avoid enabling unethical practices

LEADERSHIP – SUPPORT LIFELONG LEARNING

- Provide education on ethics and professionalism
- Familiarize staff with system impacts
- Encourage skill and judgment development

LEADERSHIP – MANAGING SYSTEM CHANGES

- Plan changes carefully
- Avoid harmful deprecation
- Support migration to alternatives

LEADERSHIP – STEWARDSHIP OF INTEGRATED SYSTEMS

- Monitor societal integration
- Ensure fair system access
- Develop new care standards as needed

COMPLIANCE – UPHOLD AND PROMOTE THE CODE

- Act consistently with ethical principles
- Encourage ethical behavior in others
- Report violations appropriately

COMPLIANCE – ACM MEMBERSHIP RESPONSIBILITY

- Support Code adherence across the profession
- Report breaches to ACM if needed
- Recognize consequences of unethical conduct

CASE STUDY – MALWARE DISRUPTION

- Justified harm vs. unintended consequences
- Ethical obligations to minimize risk
- Example of Principle 1.2 and 2.8

CASE STUDY – LINKING PUBLIC DATA SETS

- Re-identification risk from data aggregation
- Privacy concerns and ERB approval
- Principles 1.6, 2.4, and 2.5 involved

CASE STUDY – MEDICAL IMPLANT SECURITY

- Public good and proactive risk analysis
- Use of cryptography and open disclosures
- Principles 1.1, 2.9, 3.1, and 3.7 emphasized

CASE STUDY – ABUSIVE WORKPLACE BEHAVIOR

- Discrimination, abuse, and retaliation
- Leadership's ethical responsibility
- Violations of Principles 1.4, 3.3, and 3.4

CASE STUDY – BIASED CONTENT FILTERING

- Machine learning misused by activists
- Suppression of legitimate information
- Principles 1.2, 1.4, 2.5, and 3.7 relevant

USING THE CODE IN EDUCATION

- Integrate ethics into technical courses
- Use CARE framework and scenarios
- Promote critical thinking and awareness

USING THE CODE IN ORGANIZATIONS

- Adopt the Code in company policies
- Reward ethical behavior
- Encourage interdisciplinary collaboration

CONCLUSION

- The Code supports technical and ethical excellence
- Follow principles to benefit society and profession
- Uphold accountability and transparency in computing

REFERENCES

- ACM Code of Ethics and Professional Conduct (2018)
- https://www.acm.org/code-of-ethics