

SOCIAL RESPONSIBILITIES OF ENGINEERS

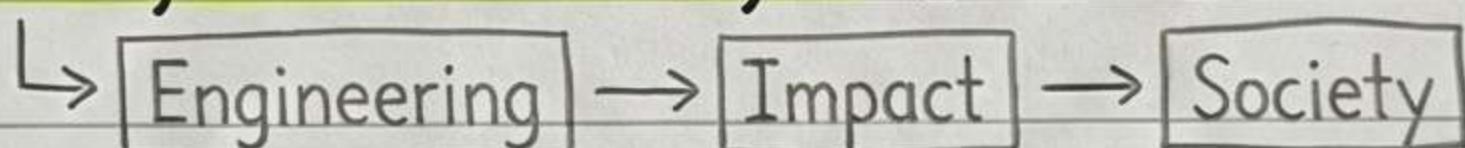
MEANING:

- Commitment to place ==public safety== & ==public interest== ahead of all other considerations [cite: 2].
- Individual engineers ==share this responsibility== [cite: 2].



4 KEY AREAS (SHORT DESCRIPTION) [cite: 1]:

1. Security: Ensure work does not ==endanger public safety==. Designs should ==protect people from harm== [cite: 1].
2. Accessibility: Consider ==needs of society== as a whole. Tech should be ==usable and beneficial== for general public [cite: 1].
3. Responsibility: Accountable for ==consequences== of professional actions. Decisions made with ==awareness of their impact== on others [cite: 1].
4. Quality of Life: Work should ==improve human well-being==. Projects should ==positively affect society== [cite: 1].



PROFESSIONAL CONDUCT (DEEP DIVE) [cite: 2]:

- Consequences: Show due regard for ==impact== on others & society [cite: 2].
- Discover Facts: Make determined efforts to ==understand issues== related to design, development, deployment [cite: 2].
- Evaluate Outcomes: Consider ==all possible outcomes== (positive & negative) [cite: 2].

EXAMPLES [cite: 0]:

- Ensure ==safety and well-being== of public [cite: 0].
- Ensure society's ==funds and resources== are well used [cite: 0].
- Refuse to work on projects that do not follow ==engineering ethics== [cite: 0].
- Speak out publicly against threats to ==public safety== [cite: 0].
- Blow the whistle on ==illegality or wrongdoing== [cite: 0].
- Prof. societies should ==provide protection== for whistleblowers [cite: 0].
- Show concern about ==social impact== of projects [cite: 0].
- Contribute services to ==worthy, non-profit groups== [cite: 0].

SOCIAL RESPONSIBILITIES OF ENGINEERS

Key Areas (4 points)

1. Security

- Engineers must ensure that their work does not endanger public safety.
- Designs, systems, and technologies should protect people from harm.



2. Accessibility

- Engineering solutions should consider the needs of society as a whole.
- Technology should be usable and beneficial for the general public.



3. Responsibility

- Engineers are accountable for the consequences of their professional actions.
- Decisions must be made with awareness of their impact on others.

Memory Trick: R = Responsible for Results

4. Quality of Life

- Engineering work should improve human well-being.
- Projects should positively affect society and the citizenry.

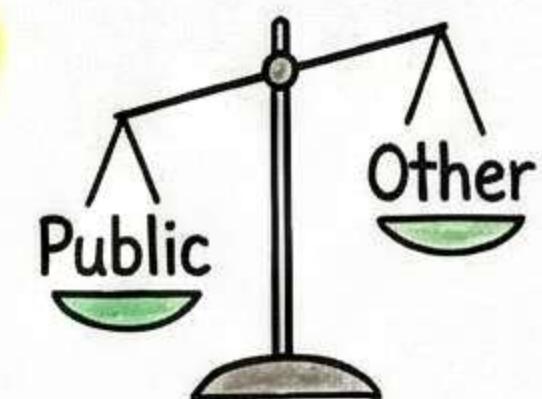


Very Imp! Exam Tip: Remember all 4 key areas.

DEEP DIVE: SOCIAL RESPONSIBILITIES OF ENGINEERS

1. Meaning of Social Responsibility.

- Commitment to place public safety and public interest ahead of all other considerations and obligations.
- Individual engineers share this responsibility.



2. Consideration of Consequences

- Must show due regard for the consequences of their conduct.
- Responsibility includes concern for:
 - The well-being of others
 - The impact of engineering work on society and citizens



3. Requirement to Discover Relevant Facts

- Must make determined efforts to:
 - Discover all relevant facts
 - Understand issues related to design, development, and deployment



4. Evaluation of Outcomes

- Must consider all possible outcomes of available choices.
- Outcomes include both:
 - Positive impacts $\oplus \uparrow$
 - Negative impacts on society and citizens $\ominus \downarrow$

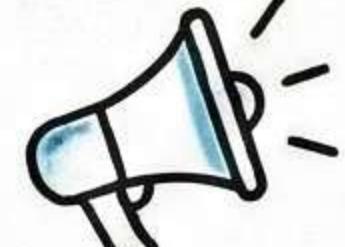
Choices → Consider → Outcomes
(+/-)

Exam Tip: Link 'Deep Dive' concepts to the 'Key Areas' for better answers!

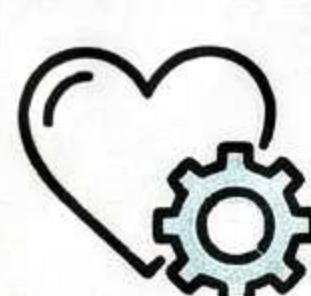
EXAMPLES OF SOCIAL RESPONSIBILITIES OF ENGINEERS

Specific Actions & Duties

- Ensure the safety and well-being of the public.
- Ensure that society's funds and resources related to technology are well used.
- Refuse to work on projects or for companies that do not follow engineering ethics.

- Speak out publicly against projects that threaten public safety.

- Blow the whistle on illegality or wrongdoing.

- Professional societies should provide protection for whistleblowers.

- Show individual and organizational concern about the social impact of engineering projects.
- Contribute services to worthy, non-profit groups and projects.


Common Mistake: Don't forget the role of professional societies!

Exam Tip:
Whistleblowing
is key!

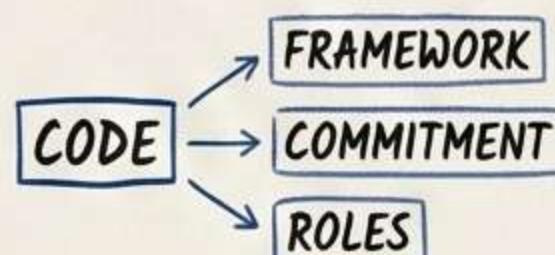
CODES OF ETHICS

What is a Code of Ethics?

- Provides a framework for ethical judgment for a professional [cite: 3].
- Expresses commitment to ethical conduct shared by profession members [cite: 4].
- Ethical codes do NOT establish new ethical principles [cite: 5].
- They reiterate principles and standards already accepted as responsible practice [cite: 6].
- Presents principles in a coherent, comprehensive, and accessible manner [cite: 7].
- Defines roles and responsibilities of professionals [cite: 8].

Types of Codes

- IEEE Code of Ethics [cite: 10].
- ACM Code of Ethics [cite: 11].



IEEE CODES OF ETHICS (short but complete) [cite: 12].

Members commit to highest conduct and agree [cite: 13]:

- To hold paramount the safety, health, and welfare of the public [cite: 14].
↳ Exam Tip: Public safety is ALWAYS priority #1! *
- To comply with ethical design and sustainable development practices [cite: 15].
- To disclose promptly factors that might endanger the public/environment [cite: 16].



- To avoid real or perceived conflicts of interest, and disclose them [cite: 17].
- To be honest and realistic in stating claims based on available data [cite: 18].
- To reject bribery in ALL its forms [cite: 19].
- To improve understanding of technology's capabilities & societal implications (incl. intelligent systems) [cite: 20].
- To maintain and improve technical competence [cite: 21].
- To undertake tasks only if qualified by training/experience, or after full disclosure [cite: 22].
↳ Common Mistake: Don't accept work you can't do without saying so!
- To seek, accept, and offer honest criticism of technical work [cite: 23].
- To acknowledge and correct errors [cite: 24].
- To credit properly the contributions of others [cite: 25].
- To treat fairly all persons [cite: 26].
- To not engage in discrimination (race, religion, gender, age, etc.)

ACM CODES OF ETHICS

1. General Ethical Principles

- Contribute to society and human well-being [cite: 33].
- Acknowledge that all people are stakeholders in computing [cite: 34].
- Be honest and trustworthy [cite: 36].
- Be fair and not discriminate [cite: 37].
- Respect work required for new ideas, inventions, creative works [cite: 38].
- Respect privacy [cite: 39].
- Honor confidentiality [cite: 40].



- To avoid real or perceived conflicts of interest, and disclose them [cite: 17].
- To be honest and realistic in stating claims based on available data [cite: 18].
- To reject bribery in ALL its forms [cite: 19].
- To improve understanding of technology's capabilities & societal implications (incl. intelligent systems) [cite: 20].
- To maintain and improve technical competence [cite: 21].
- To undertake tasks only if qualified by training/experience, or after full disclosure [cite: 22].
- To treat fairly all persons [cite: 26].
- To not engage in discrimination (race, religion, gender, age, etc.).
- To avoid injuring others, property, reputation, etc., by false/malicious action [cite: 28].
- To assist colleagues in professional development [cite: 29].
- To support others in following the IEEE code [cite: 30].

ACM CODES OF ETHICS

1. General Ethical Principles

- Contribute to society and human well-being [cite: 33].
- Acknowledge that all people are stakeholders in computing [cite: 34].
- Avoid harm [cite: 35].
- Be honest and trustworthy [cite: 36].
- Be fair and not discriminate [cite: 37].
- Respect work required for new ideas, inventions, creative works [cite: 38].
- Respect privacy [cite: 39].
- Honor confidentiality [cite: 40].



2. Professional Responsibilities

- Achieve high quality in processes and products [cite: 42].
- Maintain high standards of professional competence and ethical practice [cite: 43].
- Know and respect existing rules related to work [cite: 44].
- Accept and provide appropriate professional review [cite: 45].
- Give thorough evaluations of systems & impacts, including risk analysis [cite: 46].
- Perform work only in areas of competence [cite: 47].
↳ Memory Trick: Stay in your lane!
- Foster public awareness and understanding of computing [cite: 48].
- Access computing resources only when authorized or for public good [cite: 49].
- Design and implement systems that are robustly and usably secure [cite: 50].

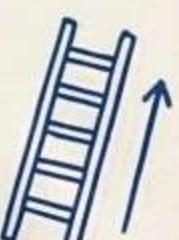
Competence

High Quality

Public Trust

3. Professional Leadership Principles

- Ensure the public good is the central concern [cite: 52].
- Encourage and evaluate social responsibilities within organizations [cite: 53].
- Manage personnel/resources to improve quality of working life [cite: 54].
- Support policies that reflect the Code's principles [cite: 55].
- Create opportunities for professional growth [cite: 56].
- Use care when modifying or retiring systems [cite: 57].
- Give special care to systems integrated into societal infrastructure [cite: 58].



4. Compliance with the Code

- Uphold, promote, and respect the Code [cite: 60].
- Treat violations as inconsistent with ACM membership [cite: 61].



CASE STUDY 1: MALWARE DISRUPTION (Rogue Services) [1]

Question focus: Which ACM Codes are violated? [cite: 2]

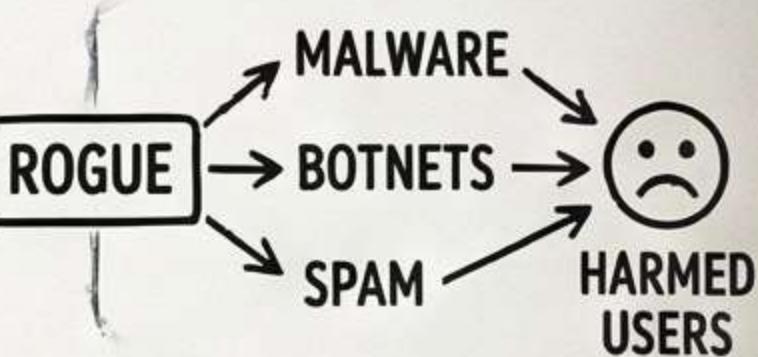
1.1 – Contribute to society and to human well-being [cite: 4]

- Rogue hosted malware, spam, botnets, and ransomware infrastructure
- These activities directly harmed society, users, and victims [cite: 6]
- Instead of contributing, they enabled large-scale cyber harm [cite: 7]

→ Violation of ACM 1.1 [cite: 8]

1.2 – Avoid harm [cite: 9]

- Rogue knowingly allowed:
 - Ransomware infections
 - Fraud
 - Exploitation of browser vulnerabilities [cite: 10, 11, 12, 13]
- Harm was predictable, continuous, and unjustified [cite: 14]
- Rogue refused to mitigate harm despite repeated warnings [cite: 15]



→ Violation of ACM 1.2 [16]

1.3 – Be honest and trustworthy [cite: 17]

- Marketing slogan: "Guaranteed uptime, no matter what" [cite: 18]
- This commitment ignored ethical consequences and misrepresented responsible conduct [cite: 19]
- Continued service despite known abuse undermines trustworthiness [cite: 20]

→ Violation of ACM 1.3 [21]



2.3 – Know and respect existing rules [cite: 22]

- Rogue exploited weak national laws to justify inaction [cite: 23]
- ACM ethics require challenging unethical rules, not hiding behind legality [cite: 24]

→ Violation of ACM 2.3 [25]

3.1 – Ensure public good is central [cite: 26]

- Rogue prioritized: Business guarantees
- Customer commitments over public safety [cite: 27, 28, 29]
- Public good was not central [cite: 30]

→ Violation of ACM 3.1 [31]



3.2 – Articulate social responsibilities [cite: 32]

- Leadership refused to act against abuse [cite: 33]
- No effort to discourage unethical use [cite: 34]

→ Violation of ACM 3.2

4.1 – Uphold the Code [cite: 36]

- Actions contradict core ACM principles [cite: 37]
- No corrective action taken [cite: 38]

→ Violation of ACM 4.1 [39]

Summary (Case 1) [cite: 40]

Violated ACM Codes: 1.1, 1.2, 1.3, 2.3, 3.1, 3.2, 4.1 [cite: 41]

★ Exam Tip: This is a "Total Failure" case!

CASE STUDY 2: MEDICAL IMPLANT RISK (Corazón) [cite: 42]

Important: Focus on ethical compliance, not violation [cite: 43]

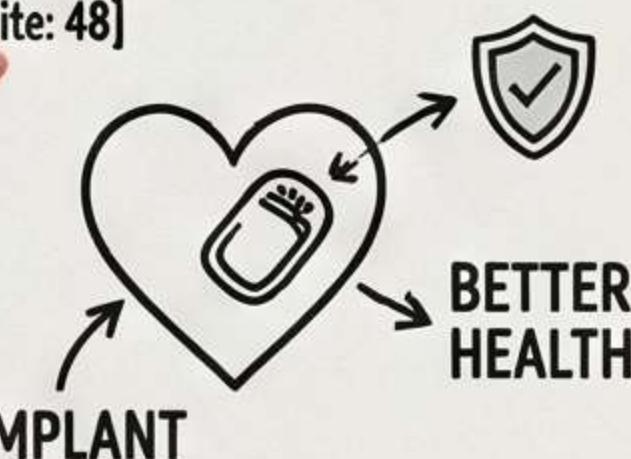
1.1 – Contribute to society [cite: 45]

- Implant improves heart health [cite: 46]

- Free/reduced access for low-income patients [cite: 47]

→ NOT violated (ethically aligned) [cite: 48]

★ Memory Trick: Corazón = Heart!



1.2 – Avoid harm [cite: 49]

- Security controls:

- Short-range access
- Encryption [cite: 50, 51, 52]

- Vulnerability had limited scope and negligible harm [cite: 53, 54, 55]

→ NOT violated [56]



1.3 – Be honest and trustworthy [cite: 57]

- Open bug bounty program [cite: 58]
- Transparent discussion with researcher [cite: 59]

→ NOT violated [60]

2.5 – Give comprehensive evaluations [cite: 61]

- Vulnerability evaluated jointly with leaders [cite: 62]
- Risk assessed before deciding [cite: 63]

→ NOT violated [64]

2.9 – Design secure systems [cite: 65]

- Encryption and cryptographic protection [cite: 66]
- Security design considered realistic threat model [cite: 67]

→ NOT violated [68]

3.1 – Public good is central [cite: 69]

- Patient safety and benefit prioritized [cite: 70]
- No concealment [cite: 71]

→ NOT violated [72]



Summary (Case 2) [cite: 73]

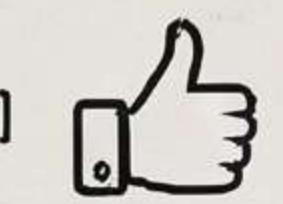
- No ACM Code violations [cite: 74]
- Ethical compliance with ACM standards [cite: 75]



Final Exam-Ready Comparison

Case 1: Multiple ACM Code violations [cite: 77]

Case 2: Ethical compliance with ACM Code [cite: 78]



Ethical Violations by Mr. Z (ACM Code) [cite: 25]

↳ "Mr. Z violated ACM Code by continuing military drone software work despite serious risks & withholding info" [cite: 26].

1. Avoid Harm & Be Honest (ACM 1.2, 1.3)

- ACM 1.2 – Avoid Harm [cite: 27]: Knew drones could misclassify targets in fog, low light, sudden movement [cite: 28].
 - In military context, could lead to civilian casualties [cite: 29].
 - Continuing work despite foreseeable life-threatening harm is a violation [cite: 30].
- ACM 1.3 – Be Honest [cite: 31]: Knowingly omitted critical limitations of software in briefings [cite: 32].
 - Lack of full disclosure misled decision-makers [cite: 33].



2. Competence & Evaluations (ACM 2.5, 2.6)

- ACM 2.5 – Comprehensive Evaluations [cite: 34]:
 - Failed to provide complete risk evaluation for high-risk military environments [cite: 35].
 - Known risks not properly communicated [cite: 36].
- ACM 2.6 – Work in Area of Competence [cite: 37]:
 - Software was for agricultural use, not military [cite: 38].
 - Working without ensuring suitability for high-risk domain = violation [cite: 39].



3. Public Good (ACM 3.1)

- ACM 3.1 – Ensure Public Good [cite: 40]: Prioritized job security and performance bonuses over public safety [cite: 41].
 - Civilian well-being was not central concern [cite: 42].

Conclusion [cite: 43]

- Mr. Z violated ACM Codes 1.2, 1.3, 2.5, 2.6, 3.1 by neglecting risk disclosure, professional responsibility, & public safety [cite: 44].

★ Exam Tip: Remember the 5 codes! Think public safety first.

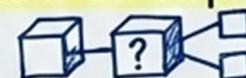
Ethical Violations by Mr. X (ACM Code) [cite: 21]

Mr. X, as Software Lead, violated ACM Code through poor leadership, misuse of authority, & neglect of responsibility. [cite: 22]

1. Privacy & Fairness (ACM 1.6, 1.4)

- ACM 1.6 – Respect Privacy [cite: 23]: Installed cameras in offices of junior developers to monitor them [cite: 24]. This was unnecessary surveillance and violated privacy/boundaries [cite: 25]. [cite: 25]. 
- ACM 1.4 – Be Fair [cite: 26]: Frequently dismissed remarks from junior developers, even though they knew the codebase [cite: 27]. → Shows unfair treatment & misuse of authority [cite: 28].

2. Competence & Growth (ACM 2.6, 2.2, 3.5)

- ACM 2.6 – Work in Area of Competence [cite: 29]: Accepted multiple blockchain projects despite having no blockchain developers [cite: 30]. → Working beyond competence [cite: 31]. 
- ACM 2.2 – Maintain Competence [cite: 32] & ACM 3.5 – Professional Growth [cite: 38]: Denied funding for an online blockchain course, calling it unnecessary [cite: 33]. Prevented skill development & failed to support team's growth [cite: 34, 39].

3. Leadership & Public Good (ACM 3.3, 3.1)

- ACM 3.3 – Enhance Quality of Working Life [cite: 35]: Enforced unpaid overtime near deadlines, affecting well-being [cite: 36]. → Degraded quality of working life [cite: 37].
- ACM 3.1 – Ensure Public Good [cite: 40]: Decisions driven by ambition for extraordinary profits, not welfare [cite: 41]. → Mismanagement harmed the company [cite: 42].

Conclusion [cite: 43]

- Mr. X violated principles of privacy, fairness, competence, leadership responsibility, & employee well-being, justifying dismissal [cite: 44].

★ Exam Tip: Leadership isn't just about profits; it's about people & ethics! Avoid Mr. X's mistakes.