Course unit: SCS 3101 - Introduction to Computer Systems

Module name/Topic: Introduction to Computer Ethics

Contributors: Selina Ochukut**,** Elisha Abade, Paul Rabala, Charles Katua, Reagan Onditi

Duration: 1 hr

Reviewed by: Selina Ochukut

Module Description

Welcome to this lesson, in this lesson, we will cover the foundational aspects of computer ethics. Computers affect every aspect of our life, and because of that, they can be used to cause harm in different ways. As computing professionals, you will have the ability to both do good and harm. This lesson will introduce you to the principles that will guide you as a computing professional to use your computing knowledge for the good of the society and the environment.

Module learning outcomes:

By the end of this lesson, the learner is should be able to;

1. State ethical principles and standards in computer ethics
2. Explain the importance of computer ethics
3. Apply the different ethical principles in different computing environments
4. Evaluate different scenarios to identify ethical issues

Topic/Module contents:

1. **Introduction**

The actions of a computing professional can change the world, as a computing professional, you will need to think about what impacts your actions will have.

Warm up

What is your understanding of ethics?

Students to give their views of what they think ethics is

Ethics are standards and principles that guide people on how they should behave or live. They are not like laws that are to be strictly adhered to but for the benefit of society, it is important that they are followed. Ethics helps us in distinguishing what is right and wrong.

What ethics is not

As we think about ethics, let's do so by describing what ethics is not; this section highlights a few things that ethics is not.

1. **Ethics is not what one feels to be right or wrong**. A person's feeling may make them not do what is ethical. In many instances, peoples' feelings deviate from what is ethical.

2. **Ethics cannot be equated with following the law**. In some instances the law deviates from what is supposed to be ethical. E.g ..
3. **Ethics cannot be equated to what the society accepts** because of the fact that one cannot get consensus on what is ethical or not.

What is computer ethics

Now that we have looked at what ethics is and what it is not, let's talk about what computer ethics is. Computer ethics can be defined as principles that govern the proper use of computers or computing devices. It can be described as a set of moral principles whose major aim is behavior influence so as to avoid harm.

Class discussion

Why do you think it is important to talk about computer ethics?

Some of the reasons why we need computer ethics are;

1. Increased cyber crimes cases: Almost on a daily basis we get to hear about cases of cyber crimes in the news all over the world. Here are a few of those cases in Kenya.
   https://www.the-star.co.ke/business/kenya/2023-05-10-cybercrime-on-the-rise-as-kenya-faces-1-million-threats-everyday/
   https://www.standardmedia.co.ke/article/2000204352/agency-says-3000-cyber-crime-cases-reported-in-kenya-monthly
   8 Kenyans Among 12 Suspects Sentenced to 8 Years Over Cyber Crimes in Rwanda

   https://allafrica.com/stories/202107070174.html

2. Losses due to computer failure: There has been a lot of losses resulting from computer failure which has been attributed to computing professionals not following the ethical principles in the design and implementation of computing systems and hardware. This failure can lead to financial losses and even life.
   https://www.techrepublic.com/article/report-software-failure-caused-1-7-trillion-in-financial-losses-in-2017/
   https://www.computerweekly.com/news/450428532/Millions-being-lost-due-to-downtime-in-industrial-systems
   Describe the cases in a paragraph/ Have students search cases for the issues mentioned

As we can see from the above section, computer ethics is key to mitigating some of this losses. In the next section, we are going to look at some of the guiding principles that will help computing professions such as yourselves to make decisions that can prevent losses.

2. Professional Ethics

What are professional Ethics?

Professional ethics encompass the personal and corporate standards of behavior expected of professionals.

Professionals and those working in acknowledged professions exercise specialist knowledge and skill. How the use of this knowledge should be governed when providing a service to the public can be considered a moral issue and is termed as "professional ethics".

Professional Ethics includes: honesty, trustworthiness, transparency, accountability, confidentiality, objectivity, respect, obedience to the law, and loyalty.

Code of ethics and professional conduct in the field of computing:

Code of ethics are guidelines that guide computing professionals to make ethical decisions. In this section, we are going to highlight the different code of ethics and professional conduct that associations such as ACM and IEEE have provided.

The ten commandments of computer ethics

The ten commandments of computer ethics were provided by the computer ethics institute. They are as follows;

1. Do not use computers in ways that may harm others
2. Do not use computer technology to cause interference in other users' work
3. Do not spy on another person's computer data
4. Do not use computer technology to steal information
5. Do not contribute to the spread of misinformation using computer technology
6. Refrain from copying software or buying pirated software. Pay for software unless it is free
7. Do not use someone else computer resources unless authorized to
8. It is wrong to claim ownership of work which is the output of someone else's intellect.
9. Before developing software, think of the social impact it may have
10. In using computers for communication, be respectful and courteous with fellow members. (Wright, 2008)

3. **General ethical principles: ACM;**

1. Contribute to human well being and the society, acknowledging the stakeholders in computing includes all people: According to this principle computing professions are required to make use of their computing skills for the benefit of the society, its members and the environment. It involves human right protection and human autonomy. (Benefincense)

2. Avoid harm: harm can include unjustified physical or mental injury, unjustified disclosure of information (non-malfeasance). Computing professionals are required not to use their knowledge and skills to cause harm.
3. Be honest and trustworthy: A computing professional should be transparent and provide full disclosure of all pertinent system capabilities, limitations, and potential problems to the appropriate parties. Making deliberately false or misleading claims, fabricating or falsifying data, offering or accepting bribes, and other dishonest conduct are violations of the Code.
4. Be fair and take action not to discriminate: Computing professionals should foster fair participation of all people, including those of underrepresented groups. Prejudicial discrimination on the basis of age, color, disability, ethnicity, family status, gender identity, labor union membership, military status, nationality, race, religion or belief, sex, sexual orientation, or any other inappropriate factor is an explicit violation of the Code. Harassment, including sexual harassment, bullying, and other abuses of power and authority, is a form of discrimination that, amongst other harms, limits fair access to the virtual and physical spaces where such harassment takes place.
5. Respect the work required to produce new ideas, inventions, creative works, and computing artifacts: Computing professionals should therefore credit the creators of ideas, inventions, work, and artifacts, and respect copyrights, patents, trade secrets, license agreements, and other methods of protecting authors' works.
6. Respect privacy: Technology enables the collection, monitoring, and exchange of personal information quickly, inexpensively, and often without the knowledge of the people affected. Therefore, a computing professional should become conversant in the various definitions and forms of privacy and should understand the rights and responsibilities associated with the collection and use of personal information.
7. Honor confidentiality: Computing professionals are often entrusted with confidential information such as trade secrets, client data, nonpublic business strategies, financial information, research data, pre-publication scholarly articles, and patent applications. Computing professionals should protect confidentiality except in cases where there is evidence of the violation of law, of organizational regulations, or of the Code. In these cases, the nature or contents of that information should not be disclosed except to

appropriate authorities. A computing professional should consider thoughtfully whether such disclosures are consistent with the Code.

Professional responsibilities (ACM)

Strive to achieve high quality in both the processes and products of professional work: Computing professionals should insist on and support high quality work from themselves and from colleagues. The dignity of employers, employees, colleagues, clients, users, and anyone else affected either directly or indirectly by the work should be respected throughout the process. Computing professionals should respect the right of those involved to transparent communication about the project. Professionals should be cognizant of any serious negative consequences affecting any stakeholder that may result from poor quality work and should resist inducements to neglect this responsibility.

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

High quality computing depends on individuals and teams who take personal and group responsibility for acquiring and maintaining professional competence. Professional competence starts with technical knowledge and with awareness of the social context in which their work may be deployed. Professional competence also requires skill in communication, in reflective analysis, and in recognizing and navigating ethical challenges. Upgrading skills should be an ongoing process and might include independent study, attending conferences or seminars, and other informal or formal education. Professional organizations and employers should encourage and facilitate these activities.

Know and respect existing rules pertaining to professional work.

"Rules" here include local, regional, national, and international laws and regulations, as well as any policies and procedures of the organizations to which the professional belongs. Computing professionals must abide by these rules unless there is a compelling ethical justification to do otherwise. Rules that are judged unethical should be challenged. A rule may be unethical when it has an inadequate moral basis or causes recognizable harm. A computing professional should consider challenging the rule through existing channels before violating the rule. A computing professional who decides to violate a rule because it is unethical, or for any other reason, must consider potential consequences and accept responsibility for that action.

Accept and provide appropriate professional review.

High quality professional work in computing depends on professional review at all stages. Whenever appropriate, computing professionals should seek and utilize peer and stakeholder review. Computing professionals should also provide constructive, critical reviews of others' work.

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. Computing professionals should strive to be perceptive, thorough, and objective when evaluating, recommending, and presenting system descriptions and alternatives. Extraordinary care should be taken to identify and mitigate potential risks in machine learning systems. A system for which future risks cannot be reliably predicted requires frequent reassessment of risk as the system evolves in use, or it should not be deployed. Any issues that might result in major risk must be reported to appropriate parties.

Perform work only in areas of competence.

A computing professional is responsible for evaluating potential work assignments. This includes evaluating the work's feasibility and advisability, and making a judgment about whether the work assignment is within the professional's areas of competence. If at any time before or during the work assignment the professional identifies a lack of a necessary expertise, they must disclose this to the employer or client. The client or employer may decide to pursue the assignment with the professional after additional time to acquire the necessary competencies, to pursue the assignment with someone else who has the required expertise, or to forgo the assignment. A computing professional's ethical judgment should be the final guide in deciding whether to work on the assignment.

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

As appropriate to the context and one's abilities, computing professionals should share technical knowledge with the public, foster awareness of computing, and encourage understanding of computing. These communications with the public should be clear, respectful, and welcoming. Important issues include the impacts of computer systems, their limitations, their vulnerabilities, and the opportunities that they present. Additionally, a computing professional should respectfully address inaccurate or misleading information related to computing

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 other principles in the Code. Consequently, computing professionals should not access another's computer system, software, or data without a reasonable belief that such an action would be authorized or a compelling belief that it is consistent with the public good. A system being publicly accessible is not sufficient grounds on its own to imply authorization. Under exceptional circumstances a computing professional may use unauthorized access to disrupt or inhibit the functioning of malicious systems; extraordinary precautions must be taken in these instances to avoid harm to others.

Design and implement systems that are robustly and usably secure.

Breaches of computer security cause harm. Robust security should be a primary consideration when designing and implementing systems. 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. As threats can arise and change after a system is deployed, computing professionals should integrate mitigation techniques and policies, such as monitoring, patching, and vulnerability reporting. Computing professionals should also take steps to ensure parties affected by data breaches are notified in a timely and clear manner, providing appropriate guidance and remediation.

4. Professional leadership principles (ACM)

1. Ensure that the public good is the central concern during all professional computing work
2. Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.
3. Manage personnel and resources to enhance the quality of working life.
4. Articulate, apply, and support policies and processes that reflect the principles of the Code
5. Create opportunities for members of the organization or group to grow as professionals
6. Use care when modifying or retiring systems.
7. Recognize and take special care of systems that become integrated into the infrastructure of society.

Cases

Case 1/ *use african names like Omanyala, Kipchonge, Kerubo,*

Adrian works as an intern in a small company called Millenium that offers short courses on different IT subjects. He is tasked with the job of ensuring that all the computers at Companies lab have installed softwares and hardware required for the various courses the students are undertaking. In the process of installing the operating systems, Adrian realizes that the company's licensed OS is not the current one in the market and is not compatible with the softwares that students require for their practicals. Adrian calls his friend who is interning in another organization and the friend offers Adrian a licenced OS from the organization he works in. Adrian goes ahead and installs the OS he got from the friend without consulting his supervisor.

1. What are the ethical issues arising from this case?

Case 2

Marlin, a recent graduate from the University of Nairobi's Bsc. Computer Science program applied for a consulting job at Kalib tech. In the application, Marlin had indicated that he had expertise in cyber security even though marlin had no knowledge in cyber security. The company invited Marlin for an interview and because they did not have any expert in cybersecurity in the panel to evaluate Marlin's competencies, they ended up hiring her. Marlin is tasked with the job of ensuring that all the applications developed are secure and are not prone to attack. Within the first three months on the job, the company experiences a cyber-attack, and the customer data in one of the systems got exposed. During the meeting, to evaluate the impact, Marlin was not able to explain why the breach happened and how they can control the impact of the breach.

1. What ethical principles did Marlin ignore in this case?
2. Were Marlin’s actions ethical?

Assignments /Quizzes:

1. Which of the following is not part of the ten commandments of ethics
   a. Do not kill
   b. Do not spy on another person's computer data
   c. Do not use computer technology to steal information
   d. Do not contribute to the spread of misinformation using computer technology

   Answer: a
2. Martin was assigned a data science job. When evaluating the job, Martin realized he did not have the necessary skills to finish the project. Instead of letting his boss know, Martin contracted his friend to do the job and paid him a small amount of money. According to the principles and standards of ethics that you have learned in this lesson, were Martin's actions ethical?
   a. Yes
   b. No

   Answer: No
3. Eliud owns a hardware store in Kitengela, in order to help him manage his inventory, Eliud keeps data about his customers such as names, age, physical addresses and mobile numbers. Eliuds friend has just opened a cereal shop and has requested Eliud to share his customers' details with him so that he can market his product to them for a small fee. If Eliud shares the customer information with the friend, what ACM ethical principle will he be violating? Select all that apply
   a. Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing
   b. Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing
   c. Respect privacy:
   d. Honor confidentiality

   Answer: a,c,d
4. A persons' feelings may make them make decisions that are not ethical?

   a. True
   b. False

   Answer: a

5. Which of the following are the reasons why computing professionals should learn about ethics
   a. Ethics is an interesting subject
   b. Not adhering to ethics leads can lead to huge amount of losses
   c. There is an increase in crimes committed by computing professionals world wide
   d. Learning ethics can make computing individuals obey the law

   Answers: b,c

References

1. ACM. (n.d.). ACM Code of Ethics and Professional Conduct. https://www.acm.org/code-of-ethics
2. ClassNotes. (n.d.). Computer Ethics - SS1. https://classnotes.ng/lesson/computer-ethics-3-sss1/
3. IEEE. (n.d.). IEEE Policies: Section 7 - IEEE Code of Ethics. https://www.ieee.org/about/corporate/governance/p7-8.html
4. Markkula Center for Applied Ethics. (n.d.). What Is Ethics? https://www.scu.edu/ethics/ethics-resources/ethical-decision-making/what-is-ethics/
5. University of Cape Town. (n.d.). Ethics_Top.pdf. https://www.cs.uct.ac.za/mit_notes/ethics/pdfs/ethics_top.pdf
6. Wright, C. (2008). Chapter 8—Assessing Security Awareness and Knowledge of Policy. In C. Wright (Ed.), *The IT Regulatory and Standards Compliance Handbook* (pp. 161–194). Syngress. https://doi.org/10.1016/B978-1-59749-266-9.00008-4