CSE 403
Software Engineering Professional Practice

Lecture 2
Code of Ethics and Professionalism

2025

2. Code of Ethics and Professionalism in Software Engineering

Overview of today's lecture

- Professionalism
- Nature and roles of Professional Societies
- Role of Ethics in stages of the SDLC
- Software Engineering Code of Ethics and Professional Practice
- Nature and roles of Professional Societies
- Software Engineering Standards
- Employment Contract
- Intellectual Property
- Trade-off Analysis

Professionalism

- Display of Competence of Skills expected of a profession.

- A Software Engineer displays professionalism through is the adherence to code of ethics and professional conduct to a standards and practices established by the professional community. Ie

- Computer Professionals [Registration Council] of Nigeria (CPN)
- Nigeria Computer Society
- IEEE Computer Society (IEEE CS)
- Association of Computing Machinery (ACM)
- British Computer Society etc.
    - **CPN is responsible for setting criteria for admittance and licencing activities in Nigeria**

Some Guidelines Set by these organizations

- **CPN Code of Ethics and Professional guideline**
- NITDA developed Nigeria Data Protection Regulation (NDPR) 2019
- ACM and IEEE CS have established Software Engineering Code of Ethics and Professional Practice
- ISO/IEC and IEEE have further provided internationally accepted software engineering standards
- IEEE CS has established two international certification programs (CSDA, CSDP)

Nature and Roles of Professional Societies

- Professional societies comprise a mix of practitioners and academics.
- These societies define, advance, and regulate their corresponding professions.
- Professional societies help establish professional standards as well as codes of ethics and professional conduct.

Nature and Roles of Professional Societies cont.

- They also engage in related activities, which include the following:
  - Establishing and promulgating a body of generally accepted knowledge
  - Providing the basis for licensing, certifying, and accrediting
  - Dispensing disciplinary actions
  - Advancing the profession through conferences, training, publications, and standards

Other Responsibities of these bodies

- **Accreditation**:certifies an organization's competency, authority, or credibility. A course in the University is accredited to show that it has adhere to a particular standards and maintain certain qualities. Is sometime conducted in collaboration with other private or public organizations

- **Certification & Qualification**:Professional Certification can verify the holders ability to meet profession standards through examinations etc. The qualification does not require re-qualification.
- **Licensinng**: Authorization of a person to perform certain activities and take the resultant responsibility for the product(Software)

Role of Ethics in the SDLC

Planning & Requirement Analysis

- Ensuring stakeholder needs are gathered **fairly** (no bias toward certain groups).
- Identifying potential **social impacts** (e.g., surveillance risks in data collection).
- Avoiding unethical purposes (e.g., software for illegal activities).
- **Transparency** in project goals and constraints.

System Design

- **Privacy-by-design** (data protection mechanisms).
- **Accessibility** (ensuring inclusivity for users with disabilities).
- Avoiding **dark patterns** (manipulative UI designs).
- **Security considerations** (protecting against misuse).

Role of Ethics in the SDLC cont.

Implementation (Coding)

- Writing **secure code** (avoiding vulnerabilities that could harm users).
- Avoiding **hardcoded backdoors** or unethical surveillance features.
- Ensuring **open-source compliance** (respecting licenses).
- **Bias-free algorithms** (e.g., in AI/ML models).

Testing

- **Informed consent** if testing involves real user data.
- **Fair testing** (covering diverse user scenarios, including marginalized groups).
- Avoiding **exploitative testing practices** (e.g., unpaid labor in crowdsourced testing).
- Reporting vulnerabilities **responsibly** (ethical disclosure).

•

Role of Ethics in the SDLC cont.

Deployment

- **User consent** (clear terms & conditions).
- Avoiding **forced updates** or deceptive deployment practices.
- Ensuring **equitable access** (not excluding certain regions or groups).
- **Environmental impact** (energy-efficient deployment).

Maintenance & Suppo

- Providing **timely security patches** to protect users.
- **Transparency** about data collection in updates.
- **Fair pricing** (no exploitative subscription models).
- **Handling user data responsibly** (NDPR, GDPR, CCPA compliance).
-

Role of Ethics in the SDLC cont.

Retirement/Decommissioning

- **Ethical Considerations:**
  - **Secure data disposal** (preventing leaks of old user data).
  - **Informing users** about discontinuation and migration options.
  - **Environmental responsibility** (e-waste management).

Key Ethical Principles Across SDLC:

1. **Accountability** (taking responsibility for software impact).
2. **Transparency** (clear communication with stakeholders).
3. **Fairness** (avoiding bias and discrimination).
4. **Privacy & Security** (protecting user data).
5. **Sustainability** (minimizing environmental harm).

Software Engineering Code of Ethics and Professional Practice

- Software engineers shall commit themselves to making the analysis, specification, design, development, testing and maintenance of software a beneficial and respected profession.
-
    - Joint Effort by IEEE-Computer Society and Association of Computing Machinery(ACM)

Software Engineering Code of Ethics and Professional Practice

- In accordance with their commitment to the health, safety and welfare of the public, software engineers shall adhere to the following Eight Principles:

Software Engineering Code of Ethics and Professional Practice cont.

- 1. **PUBLIC** – Software engineers shall act consistently with the public interest.
- 2. **CLIENT AND EMPLOYER** – Software engineers shall act in a manner that is in the best interests of their client and employer consistent with the public interest.
- 3. **PRODUCT** – Software engineers shall ensure that their products and related modifications meet the highest professional standards possible.
- 4. **JUDGMENT** – Software engineers shall maintain integrity and independence in their professional judgment.
- 5. **MANAGEMENT** – Software engineering managers and leaders shall subscribe to and promote an ethical approach to the management of software development and maintenance.
- 6. **PROFESSION** – Software engineers shall advance the integrity and reputation of the profession consistent with the public interest.
- 7. **COLLEAGUES** – Software engineers shall be fair to and supportive of their colleagues.
- 8. **SELF** – Software engineers shall participate in lifelong learning regarding the practice of their profession and shall promote an ethical approach to the practice of the profession.
-

Nature and roles of Professional Societies

- The Professional Society is comprised of practitioners and acdemics alike. These societies define, advance and regulate the profession.
- **Roles or Activities**:

1. Establishing and promulgating a body of generally accepted knowledge(Like this course)
2. Provide the basis for licensinng, certifying and accreditig.
3. Dispensing disciplinary actions.
4. Advancing the profession through conferences, training, publications and standards.

Software Engineering Standards

- Software engineering standards provide guidelines for the practice of software engineering and for the processes to be used in the software development lifecycle.
- **Example**
- Guidelines for software development by NITDA provides a minimum requirement for the development of software to be used in Nigerian government entities. Ensuring Quality, Security and operational standards.
- ISO/IEC/IEEE software enginering standards mostly on documenting. Like ISO/IEC/IEEE 15288:2015
- **Usually, adherance to standard promotes dicipline in the profession**.

Employment Contract

- Software engineering services may be provided in a variety client – engineer relationship
  - Company to Customer
  - Engineer to Customer
  - Direct hire
  - volunteering

Employment Contract (Engineer to Customer)

- Concerns with software enginnering contracts:
  - Confidentiality?
  - Ownership Rights?

Employment Contract (Engineer to Customer) Cont.

- Most employers derive value through intellectual property(IP).
- Most Employers will require software engineers to sign a non-disclosure agreements(NDA) or IP agreements as precondition for working with them.
- IP Ownership: the right to the assets(product, innovations, inventions,discoveries and ideas) are explicitly stated in the contract terms

Employment Contracts cont.

- **Employment Contract should contain but not limited to :**
  - Location of work
  - Standard of work
  - System configuration for development
  - Limitations of both party liabilities
  - Communication matrix and escalation plan
  - Rates
  - Frequency of compensation (hourly,daily, weekly, monthly, project based)
  - Working hours
  - Working conditions etc.

Intellectual Property (IP)

- refers to creations of the mind, such as inventions, literary and artistic works, designs, and symbols, names, and images used in commerce
- Types of Intellectual Property
  - Copyright
  - Trademark
  - Patents
  - Trade Secrets

Intellectual Property (IP):Copyright

- Copyrights protect the way an idea is presented usually for a limited time.
- Not the idea itself
  - **For example**, copyright may protect the particular wording of an account of an historical event, whereas the event itself is not protected.

Intellectual Property (IP): Trademarks

- A trademark relates to any word, name, symbol, or device that is used in business transactions. It is used “to indicate the source or origin of the goods”
  - Trademark protection protects names, logos, images, and packaging. However, if a name, image, or other trademarked asset becomes a generic term, then trademark protection is nullified
  - World Intellectual Property Organization (WIPO) is the authority that frames the rules and regulations on trademarks.

Intellectual Property (IP):Trademarks (Cont.)

Intellectual Property (IP): Patents

- Patents protect an inventor's right to manufacture and sell an idea. A patent consists of a set of exclusive rights granted by a sovereign government to an individual, group of individuals, or organization for a limited period of time. It is an idea-ownership protection.
  - Application for a patent entails careful records of the process that led to the invention
  - **Note that,** if inventions are made during the course of a software engineering contract, ownership may belong to the employer or customer or be jointly held, rather than belong to the software engineer.
  - There are rules concerning what is and is not patentable.
  - In many countries, software code is not patentable, although software algorithms may be.
  - Existing and filed patent applications can be searched at WIPO.

Intellectual Property (IP): Trade Secrets

- an intellectual asset such as a formula, algorithm, process, design, method, pattern, instrument, or compilation of information not generally known that may provide a business some economic advantage.
  - “trade secret” provides legal protection if the asset is stolen.
  - This protection is not subject to a time limit
  - However, if another party derives or discovers the same asset legally, then the asset is no longer protected and the other party will also possess all rights to use it.

Professional Liability

- As an individual provides services to a client or employer, it is vital to adhere to standards and generally accepted practices, thereby protecting against allegations or proceedings of or related to malpractice, negligence, or incompetence.
  - Under the laws and rules governing in their jurisdiction, engineers may be held to account for failing to fully and conscientiously follow recommended practice; this is known as “negligence.”
  - Legal suits for liability can be brought under tort law in the US allowing anyone who is harmed to recover their loss even if no guarantees were made.Because it is difficult to measure the suitability or safety of software, failure to take due care can be used to prove negligence on the part of software engineers.
  - **How to protect your self**
  - A defense against such an allegation is to show that standards and generally accepted practices were followed in the development of the product.

Legal Requirements

- Software engineers must operate within the confines of local, national, and international legal frameworks.
  - Example:
  - registration and license (CPN Individual or Business)
  - contractual agreements
  - noncontractual legalities, such as those governing liability;

Trade Compliance

- Software professionals must be aware of legal restrictions on import, export, or reexport of goods, services, and technology in the jurisdictions in which they work
  - export controls and classification
  - transfer of goods
  - acquisition of necessary governmental licenses for foreign use of hardware and software
  - services and technology by sanctioned nation
  - enterprise or individual entities
  - import restrictions and duties

Cybercrime

- Cybercrime refers to any crime that involves a computer, computer software, computer networks, or embedded software controlling a system.
  - The computer or software may have been used in the commission of a crime or it may have been the target.
  - **This category of crime includes** fraud, unauthorized access, spam, obscene or offensive content, threats, harassment, theft of sensitive personal data or trade secrets, and use of one computer to damage or infiltrate other networked computers and automated system controls.

Cybercrime (Cont.)

- Computer and software users commit fraud by altering electronic data to facilitate illegal activity.
- Forms of Unauthorized access:
  - Hacking
  - Eavesdropping
  - using computer systems in a way that is concealed from their owners.
- software engineer has a professional obligation to consider the threat of cybercrime and to understand how the software system will protect or endanger software and user information from accidental or malicious access, use, modification, destruction, or disclosure.

Documentation

- Providing clear, thorough, and accurate documentation is the responsibility of each software engineer. The adequacy of documentation is judged by different criteria based on the needs of the various stakeholder audiences
- Good documentation complies with accepted standards and guidelines.
- **Software engineers should document**
  - relevant facts,
  - significant risks and tradeoffs
  - warnings of undesirable or dangerous consequences from use or misuse of the software
- **Software engineers should avoid**
  - certifying or approving unacceptable products,
  - disclosing confidential information, or
  - falsifying facts or data.

Documentation (Cont.)

- **Software engineers should share with their team**
  - software requirements specifications, software design documents, details on the software engineering tools used, software test specifications and results, and details on the adopted software engineering methods;
  - problems encountered during the development process.
- For **external stakeholders (customer, users, others)**
  - information needed to determine if the software is likely to meet the customer's and users' needs,
  - description of the safe, and unsafe, use of the software,
  - description of the protection of sensitive information created by or stored using the software, and
  - clear identification of warnings and critical procedures.
-

Trade-off Analysis

- Trade-off analysis is a method that involves comparing, prioritizing, and selecting among different options based on their advantages and disadvantages:
- Steps
  - Define the problem
  - Generate Alternatives
  - Evaluate Alternatives
  - Compare Alternatives
- Other things to consider
  - Monetary cost
  - Performance
  - Etc
- A software engineer must conduct a tradeoff analysis in an ethical manner

Data Privacy

- Data Protection refers to the mechanisms, tools and procedures an organization put in place to control and prevent unauthorized access to the personally identifiable information shared with them by a data subject.

Defination of some terms in Nigerian Data Protection

- **Data Subject** – This refers to any natural person, who can be identified, directly or indirectly.
- **Personal Identifiable Information (PII)** – This means information that can be used to identify, contact, or locate an individual.
- **Data Subject Access Request** – This allows for an individual to request a copy of their data through a formal process.
- **Consent** – This means any freely given, specific, or a clear affirmative action which signifies agreement to the processing of Personal Data of an individual.
- **Data Controller** – This refers to a person or a statutory body that determines the purposes and the manner in which Personal Data should be collected and processed.
- **Data Processor** – An individual or organization who processes and store data in accordance to data controller's instruction.
- **Processing**– This refers to any operation or set of operations which is performed on personal data. Whether or not by automated means, such as collection, recording, alteration, erasure or deletion.
- **Data Protection Compliance Organization (DPCO)** – This refers to any organization duly licensed by NDPC for the purpose of training, auditing, consulting and rendering services and products for the purpose of compliance with the NDPA.