Legal & Ethical Issues in ICT

By:

Dr. John K. Tarus

School of Information Sciences

INF 411/CMM 213: MANAGEMENT OF ICT

Ethical Issues in ICT

- **Ethics** refers to the principles of right and wrong that individuals use to make choices or to guide their behavior.
  - ✓ Rules for distinguishing between right and wrong.
- ICT and information systems raise new ethical questions for both individuals and societies.
- Along with the benefits of a digitally connected world comes the threats of misuse and abuse.
- ICT can be used to commit crimes and threaten social values.

Ethical Issues in ICT

- Many of the ethical issues that face ICT professionals and MIS users involve issues of privacy, copyright, computer crime and abuse, confidentiality etc.

- Countries and institutions are building mechanisms and laws to protect their people against threats of misuse and abuse of ICT e.g Computer Misuse and Cybercrimes Act 2018, Data Protection Act 2019, National Cybersecurity Strategy in Kenya etc.

- This is largely focused on responsible and irresponsible use of information technology by human beings.

Legal & Ethical Implications of ICT and MIS Systems

- **Privacy (Data Protection):**

✓ ICT systems are making it very easy for governments, institutions, businesses and individuals to obtain volumes of information about individuals with or without the knowledge of the person involved e.g. information held in government databases, banks, credit card companies, hospitals etc.

✓ The individual's data should not be used to support other third party activities without the individual's consent – it is illegal and unethical.

- **Offensive or defamatory material:**

✓ All information that is made available on-line to other people must not be defamatory, discriminatory, pornographic, excessively violent, obscene, libelous, blasphemous, seditious or incite racial hatred.

✓ ICT users must not access, store, display, receive, download or transmit offensive or obscene material as this is considered illegal and unethical.

- **Confidentiality:**

✓ ICT systems managers should ensure confidentiality and privacy of user accounts, electronic mail and any data stored by the users in the institution's or organization's databases and servers.

Legal & Ethical Implications of ICT and MIS Systems

- **Computer Crime and Abuse:**

✓ ***Computer Crime*** refers to the commission of illegal acts through the use of a computer or against a computer system e.g hacking, phishing & identity theft.

✓ ***Computer Abuse*** is the commission of acts, involving a computer which may not be illegal but are considered unethical e.g downloading big personal movies using the internet resources of your employer during official working hours, hence overloading the internet bandwidth – unethical use of computer.

✓ Most countries have in place legislation that makes computer abuse and computer crime punishable e.g Computer Misuse and Cybercrimes Act 2018.

- **Copyright and patent in software:**

✓ Computer software protected by copyright is not to be copied except as permitted by the law or by contract with the owner of the copyright.

- **ICT Users Accountability:**

✓ Individual and institutional passwords must never be shared or revealed to anyone else besides the authorized user(s).

✓ To do so exposes the authorized user to responsibility for actions the other party takes with the password.

Case Study

- Most organizations have developed their internal Acceptable Use Policies to regulate the use of ICT systems in their organizations e.g Moi University and University of Cape Town.

The following practices which are considered illegal and unethical are prohibited:

- Viewing, storing, downloading or forwarding images, videos, audio files, texts or recordings that are sexually explicit or sexually suggestive, racist, harassing, intimidating or defamatory is prohibited, except where there is both legal and there is demonstrable academic need to access or distribute such content;
- Hacking in any form, including gaining or attempting to gain access to restricted resources inside or outside of the University's computer network;
- Impersonating another user or another person;
- Obtaining without authorization the access codes and/or passwords of another user;
- Software piracy, or other infringement of intellectual property rights in digital content;
- The sending, whether on the internal email system or externally, of bulk unsolicited mail, commercial advertising of other businesses, mail-flooding, or excessive cross postings on newsgroups (called spam);
- Issuing of unsolicited e-mail to indicate or gain support for any religious or political purposes.

END

Thank You

Q & A ?