

UNETHICAL PRACTICES IN INFORMATION AND COMMUNICATION TECHNOLOGY (ICT) IN NIGERIAN HIGHER EDUCATION INSTITUTIONS

BY

Emmanuel O. Olabimitan
Dept of Computer Science Education , School of Secondary Education (Science),
FCET Bichi, Kano,
olabimitandare@yahoo.com,

Joseph Yongo Tyolumun,
Dept of Computer Science Education School of Secondary Education (Science)
FCET Bichi, Kano
tyolumunyongo@gmail.com

&

Muhammad Aminu Umar
Dept of Computer Science Education School of Secondary Education (Science)
FCE(T) Bichi, Kano
muhamiumar@gmail.com

ABSTRACT

In response to growing pressure to prepare children for life in a digital world, schools have engaged in wide scale integration of information and communication technologies (ICT) into classrooms. The use of the Internet, assistive technologies, learning management systems and mobile technologies has become a central component of educational practices reflecting a broader social dependence on digital technologies and the desire of the educational community to utilize ICT as a tool to enhance learning. However, unethical practices have seriously undermined the provision of quality and sustainable education in Nigeria. The use of ICT in education has given birth to a host of legal and ethical issues in Nigeria. This is borne out of the fact that overall goals of the education sector as enunciated in the National policy on education can hardly be achieved by stakeholders without a strict adherence to laid down rules and regulations. This paper critically xrayed unethical practices in ICT that have bedeviled our education system in Nigeria. Several ethical issues such as plagiarism, hacking, cyber-bullying, and piracy amongst others were identified as major ethical issues related to ICT. The paper also postulated that policing ICT use through acceptable policies, Internet safety education, content filter software, amongst others are measures and strategies required for global information to be exploited in a socially and ethically sensitive way for our future benefit and application.

Key words: Unethical Practices, Information and Communcation Technology, National Policy on Education,

Introduction

Education in Nigeria is nationally conceptualized not simply as the medium for cultural transmission but the main vehicle for accelerating individual, community and national development. It is a mechanism through which the society generates the knowledge and skills required for its survival and sustenance. It enriches people's understanding of themselves and the world. It improves the quality of lives and leads to broad social benefits to individuals and society (Kazeem and Ige, 2010).

Ethics on the other hand refers to the moral principles that govern the behaviour of a person or group. The notion of ethics is regularly drawn upon in the context of expected patterns of behavior written or unwritten, consistent with generally accepted standards for those to whom it may concern. However, there are various perspectives on the concept of ethics. Floridi & Sanders (2001) defined the concept as an individual's personal belief about what is right or wrong, good or bad. On a counter side, Johnson (2000) defined ethics as right or wrong actions that stems from the value and expectation of society. Forester & Morrison (2007) notes that ethics are acceptable standards of behaviour that define how people ought to act (prescriptive) not how people really act (descriptive).

In the context of an operational definition with regards to professions, ethics generally refers to those principles and codes of behaviour that guide the conduct of any profession. The term usually carries along moral values, normative judgments and moral obligations. At any rate, every profession possesses its own ethics. However, there are some commonalities in professional ethics. These ethics that are common derive from the general expectations of the public from either a public officer or a professional practitioner. The issue of ethics usually goes along with allocation of value judgment such as good or bad; right or wrong.

Tavani (2003) defines the concept as an individual's personal belief about what is right or wrong, good or bad. It is the arbiter of an individual's evaluation of the "rightness" or otherwise of his or her actions. Though often regarded as subjective, it is traceable to the foundation of an individual's belief system and judged within context. Conversely, Cate (1997) notes that the ethical stance of a firm is constructed based on the expectation of society, that is, the legitimate claims made by the constituencies to whom the firm interacts. According to Agre & Rotenberg (1998), the question of ethics is one that is linked with the history of mankind. Ethics deals with the character, conduct and moral of human beings. It deals with good or bad, right or wrong behaviour. It evaluates conduct against some absolute criteria and puts negative or positive values on it. It is the reflective study of what one ought to do, or how one ought to live. Erundu, Sharland and Okpara (2004) hold that the study of "ethics" focuses on issues of practical decision making, including the nature of ultimate value and standards by which a human action can be judged right or wrong, good or bad. For Baird, et al (2000), ethics is the general term referring to both moral beliefs and ethical theory on human conduct. Ethics is a

reflection on morality. It refers to the principles of right and wrong in making choices by individuals. It has been described as the art and science that seeks to bring sensitivity and methods to the discernment of moral values (Johnson, 2000). Thus, ethics guide human and societal behavior. Tavani (2003) had no difficulty in asserting that ethics is an unending quest on explicit and implicit use of the moral code..

In other words, Ethical behavior occurs when one acts with equity, fairness and impartiality and respects the rights of others, or simply put, when one does what is morally right. while on the other hand, unethical behaviors occur when decisions enable an individual or organization to gain at the expense of the larger society (Ogunleye: 2000). Overtime, unethical practices have affected the fortunes of our educational system in Nigeria. The university system, we once prided ourselves with as citadel of learning and centre of academic excellence has joined the maddening crowd to shed its core values. “A comparison between the universities of the 1960s and 1970s with those of the past two decades will show wide disparity in terms of the quality of both the inputs and the outputs,” (Adukwu – Bolujoko,2012)

The strands of thought that readily comes to mind whenever the issue of Nigeria's educational policy is raise dare; decline in standard, deterioration of facilities, examination malpractices, mass production syndrome and the likes. Our present education system risks the chance of losing its mandate of providing qualitative education if the continuous decline in ethics is not checked. A closer look at the system reveals an entire gamut of unwholesome and unethical practices bedeviling it. The rot has permeated every facet of the education sector. It cuts across students of all ages, parents, teachers, government and the society at large. It is in view of this worrisome trend, that this paper is written to review some unethical practices associated with the use of Information and communication technology by students in tertiary institutions and how these actions have inhibited provision of quality and sustainable education in Nigeria, and their contribution to the collapsing state of Nigeria society in general.

Computer Ethics

Computer ethics is a major new field of study that addresses ethical issues in the use, development and management of information technology as well as in the formulation of general societal policies regarding the regulation of information technology in society (Johnson, 2000; Tavani, 2003; Spinello, 2000; Baird et al., 2000).

Information and communications technology (ICT) is an umbrella term that describes all the technologies that are used for the creation, transmission and modification of information. In line with this, information ethics has been defined as 'the branch of ethics that focuses on the relationship between the creation, organisation, dissemination, and use of information'.

According to Floridi & Sanders (2001), the foundation of computer ethics was laid down by Prof. Norbert Wiener, of the Massachusetts Institute of Technology, during the First World War, when he designed anti-aircraft cannons and foresaw revolutionary social and ethical consequences of information feedback systems. However, he did not use the term 'computer ethics'. That recognition goes to Walter Maner who used the term to refer to the field of inquiry that deals with ethical problems aggravated, transformed or created by computer technology. As such, ICT essentially only provides new outlets for old ethical problems (Floridi & Sanders 2001).

ICT has an increasing level of influence on the way we live, shop, work, play and learn. It essentially permeates every fabric of our lives and plays a key role in the evolution of ethics / ethical behaviour. ICT does not necessarily redefine ethics; rather it just generates new ethical issues. As our lives get further intertwined with cyberspace, it has become necessary to pay closer attention to the ethical use of ICT.

ICT professionals now have access to a lot of confidential information such as health records, GPS coordinates of transportation fleets, financial records and more. This level of access has heightened privacy concerns and privacy is considered to be one of the most important topics when it comes to the issue of ethical behaviour. (Tavani, 2008). However, with the growing incidence of cyberthreats, there is now an urgent need to balance the demand for privacy with that of security.

According to Floridi (2007), "we must be able to address and solve the ethical challenges arising in the new environment on the basis of the fundamental principles of respect for information [infosphere], its conservation and valorization". In other words, computer ethics is to deal with information privacy in ICT. Similarly, if computers and the infosphere are to be used effectively and continuously, teachers, the closest practitioners to children, are expected to teach students about the potential dangers of unethical use of technology and ethical challenges arising in the education environment.

Unethical uses of ICT in institutions of higher learning in Nigeria

The following are ethical issues arising from use of Information and Communication Technology in (higher) education in Nigeria

1.Digital Plagiarism: This is a highly unethical practice that happens so frequently, owing to free access to lots of information that is now available on the internet. Plagiarism is a term used to describe the act of taking another individual's work and claiming it to be one's own work, without any credit or reference to the original work. It is one of the major forms of academic dishonesty that has always existed in education among students and teachers. Take for instance, students in most cases copy assignment from their fellow students in part or in whole, or duplicate the existing published works especially when assignment is to be prepared electronically. Hinman,(2002) argued that plagiarism has become easier for students in two ways: "word processing programs

allow students to easily “cut and paste” information from the Internet or other electronic media to develop a paper that appears to be original work; and “students' use of Internet information that may be unavailable in traditional sources makes academic dishonesty more difficult to detect.

2. Breaking copyright and software theft (piracy): It is well known that the illegal copying of copyrighted media (texts, music works, movies and software programs) is widespread in human society. Moreover, many people who engage in such activity do not consider themselves to be doing something that is patently immoral. This immoral act is equally being practiced among students in Institutions of higher learning. Cohen and Cornwell (1989) and Glass and Wood (1996), for example, found that a large majority of students do not perceive the illegal copying of software as unethical. This attitude of students seems to match developments in the current information age, in which the Internet increasingly functions as the most important information medium that people use. Hinman (2002) has argued that the very structure of the Internet undermines the notion of private intellectual property on the web: “The inner dynamic of the Web moves us increasingly toward a much more communal notion of property”. As he explains, the Web stimulates copying because the very nature of browser technology necessitates making copies, hence, perfect copies can be made at virtually no cost, and because making digital copies does not involve physical theft from the person who owns the original. It may be added to this that many information sources on the Web are not obviously copyrighted, and many even lack an identifiable author (Kolko, 2000).

Lipinski and Britz (1999) argue, moreover, that digital copying can often be morally, if not legally, defended because of the fact that access to information is a critical need in an age of information that may in some cases override proprietary rights. Hence, the traditional legal paradigm of intellectual property is increasingly challenged by a new paradigm that emphasizes unrestrained access to, and use of, information. It is difficult to find an adequate moral compass to navigate the new landscape, not only for students, but for staff as well. But, for corporations, and software designers in particular, this is a very serious issue, and can significantly destroy profit making.

3. Hacking: A hacker is an individual who is knowledgeable enough to gain access without authorization to computer systems. Hacking is breaking into computer systems for unauthorized purposes, which may be either malicious or nonmalicious. Hacking may involve, for example, snooping around on someone's personal computer through remote access, intentionally modifying or destroying files to which one has not been granted access, releasing computer viruses, stealing passwords or files, exposing personal information and stealing electronic money (Forester & Morrison, 2007, Baase, 1997). Students and staff members at both virtual and conventional institution of learning may engage in hacking for a variety of reasons. They may simply be unaware that they are breaking into a computer system, they may just be curious, they may be out

to harm someone, they may want to benefit themselves, or they may have entirely different reasons. Malicious hacking is clearly morally problematic, but non malicious hacking has been defended by hackers as morally acceptable and socially harmless or even beneficial (Baase, 1997). Clearly, institutions of higher learning need clear policies and guidelines on hacking (including policies that define what kinds of computer system's access are unauthorized for whom) and probably need to distinguish malicious from non malicious hacking.

4. Online bullying and online harassment: The use of technology has made possible discovery of new forms of attack that transcend the school environment and enable the privacy of the bullied child or youth to be constantly invaded. Patchin & Hinduja (2006) noted that whether receivers or perpetrators are victims of various forms of online bullying (including cyberbullying, sexting, trolling, and happy slapping) that go beyond the school context and disturb their psychological and personal development. In higher institutions today, there are various electronic means of communicating messages to other members of the academic community, as well as to persons outside the school environment. E-mail, electronic bulletin boards, collaborative virtual environments and web pages constitute some of the most important ones. As in face-to-face communication, these computer-mediated forms of communication can be used to send threatening, obscene, inflammatory or harassing messages. These may include discriminatory messages used to disparage individuals or groups based on gender, race, sexual orientation, religion, age, or disability. Such messages are generally not considered to be acceptable in an academic setting, as educators strive to ensure that the classroom, if not the campus at large, functions as a safe, nonthreatening environment for students as well as for staff. In relation to this, the same principles apply for virtual classrooms and campuses as for their physical counterparts (Ferganchick-Neufang, 1997).

5. Breaches of informational privacy and confidentiality : Information privacy and confidentiality refer to access details given by users or network administrators that define access rights to files on a network. Privacy is generally considered to be an individual right in Western countries, and many nations have privacy laws (or data protection laws, as they are sometimes called in Europe). It is nowadays generally recognized that new technologies, and particularly information and communication technologies, raise new privacy issues, for example concerning electronic databases and online privacy (Cate, 1997; Agre and Rotenberg, 1998). Many of these new privacy issues can be expected to apply to the use of institutions of learning that make a lot of use of online instruction and communication. In such institutions of learning, many important activities of members of the school community can in principle be monitored or recorded electronically. This includes not only students' administration but also classroom discussion, student-to-student and student-to-lecturer, e-mail contact, and the online behavior of students in general.

The walls of classrooms and offices at such a school are much more permeable than those of classical Institutions of learning, making undercover work much easier. It happens much more frequently that the things that are said and done in them are recorded so as to be available for later scrutiny, or can be copied for distribution. At many (conventional) schools, privacy policies only put into consideration the students' privacy policies that protect a student's records from being accessed by third parties without authorization. Since many students' records are nowadays stored in electronic format, these policies must be supplemented with good system security. Electronic records should be adequately protected so as to avoid unauthorized access to them. Many higher institutions of learning nowadays also have policies that address the electronic posting of grades, which are considered to be privacy-sensitive. Many more privacy issues can be raised at any institution that has much of its communication and instruction online.

However, consider first, the confidentiality of classroom or group discussion or one-to-one and one-to-many. Can students be sure that these discussions are not logged or monitored by administrators, that they are not made accessible on public networks, and that access to them cannot be easily hacked? In a study of privacy in online learning environments, Tu (2002) argues that class discussions over a connection that is not secure may either inhibit discussion or force students to take risks in disclosing more personal information. He argues in favor of more private interaction environments, which he claims to be “key to increasing interactivity”. As he claims: “A sound learning environment will allow learners to adjust to the ideal levels of privacy and give students more secure and more comfortable environments to increase their social presence to enhance social interaction”.

6. Watching of Pornographic Videos: With the advent of almost every new media technology, pornography has been its “killer app,” or the application that drove early deployment of technical innovations in search of Pornography. Students use the internet to watch nude pictures and sex film. This act (pornography) is an abomination in Nigerian culture. The possession of free internet access to, pornographic pictures and videos by students have caused a lot of damage to sexual behavior of students on campus. Research work revealed that students that engage in watching of pornographic pictures and videos are prone to sexual immoralities as the pictures and videos make them to engage in rapping, sexual harassment, masturbation and lots of negative sexual behavior and these have remained big problems that have no easy solutions (Spinello, 2000).

Strategies for ensuring responsible use of ICT on campuses of institutions of higher learning in Nigeria for quality education

The following suggestions will help to curb unethical practices associated with ICT use in Nigeria's higher institutions:

i. Peer Assistance

It is clear that many young people know far more about life on the internet than many adults. Many young people turn a deaf ear to adults seeking to impact Internet safety education because the adult is simply "don't get it." Educators can make excellent use of the wisdom of youth. When offering Internet safety education, the more effective strategy will be for the instructor to encourage class discussion and exchange, rather than engaging in lectures. Additionally, technically-experienced students can be used as lab monitors to provide technical assistance, as well as help to ensure that students' internet use is in accord with the Internet Use Policy.

ii. Acceptable Use Policies

The most significant concern related to IUPs (Internet Use Policies) has to do with formulation of internet use policy on campus that will comprise of do's and don'ts on net. This will meet the requirements of the basic component of a comprehensive approach of a clear policy that is well-communicated to staff and students.(Children's Online Protection Commission (COPC))

iii. Internet Safety Education

This is clearly one of the most critical issues that require urgent attention on our campus. Unfortunately, in most schools there is a perception that safety concerns have been addressed by the installation of filtering. Failure to address important safety skills leaves students at greater risk and vulnerability at the inevitable times when they have access through an unfiltered system. This is the equivalence of having adult crossing guards at every crosswalk on the way to school, but failing to warn children about dangers posed by moving vehicles and the important safety skill of looking both ways prior to crossing the street.

In addition to safety education, schools need to teach students the responsible use of the Internet. These issues are two sides of the same coin. Regardless of the perception that there is no obvious forum for the introduction of this material into existing curricula, there is clearly a need for such education.

iv. Media Campaigns

There is a need for media campaign to focus on sensitization of our educational institutions to the need for installation of filtering software. As filtering software has now been recognized as the only "technology fix" there is a need for information programs that will help school Managements empower their students on campuses to make safe and responsible choices when they use the Internet.

Because schools are the universal location where young people have access to the Internet and because many parents have acquired a computer and established Internet

access at home for the purpose of supporting their children's education, it seems reasonable to conclude that schools should bear an important responsibility of helping to educate parents.

v. Institutions' Managements and Checking Unethical use of ICT: School Management should be committed to protecting academic freedom, which includes freedom of research, freedom of learning and freedom of teaching, as well as overall freedom of speech. Their policies and procedures should reflect this commitment. Also, School management should be very cautious about filtering, blocking or removing electronic information or messages, monitoring computer systems and electronic communications of students and staff, and proposing speech codes for electronic communications. If any such actions are to be taken at all, they should respect as much as possible academic and intellectual freedom as well as personal privacy.

Conclusion

In order words, the following policy recommendations may be made to School managements regarding the use of information technology in a way that respects academic freedom and free speech:

References

- Adukwu-Bolujoko.S.N.(2012) Ethics and values in the university system: The registry as an instrument of change and innovation. Being a lecture delivered at the 3rd annual lecture of the registry of the Federal University of Technology, Akure, Ondo State.
- Agre, P. & Rotenberg, M. (1998). Technology and privacy: *The new landscape*. MIT Press.
- Baird, R. M. & Ramsower, R. & Rosenbaum, S.E. (eds.) (2000). *Cyberethics*. Prometheus Books
- Cate, F. (1997). *Privacy in the information age*. Brookings Institutions Press.
- Cohen, E. & Cornwell, L. (1989). A question of ethics: Developing information system ethics. *Journal of Business Ethics* 8, 431-437.
- Floridi, L.,&Sanders, J.W. (2001). Artificial evilandthe foundation ofcomputer ethics. *Ethicsand Information Technology*, 3(1),55-66.
- Forester, T. & Morrison, P. (2007). *Computer ethics: Cautionary tales and ethical dilemmas in computing*. (2nd ed). MIT Press.
- Johnson, D. (2000). Computer ethics (3rd ed). Prentice Hall.
- Fergqnchick, B. and Neufarg, H. (1998) Bias in computer systems, In B. Friedman(Ed.),*Human values and the design of computer technology*. Cambridge University.
- Hinman, L.M. (2002). The impact of the internet on our moral lives in academia,*Ethics and Information Technology*, 4, 31-3

- Kazeem and Ige(2010), Redressing the growing concern of the education sector in Nigeria, Faculty of Education, University of Benin.
- Kolko, B. (2000). 'Intellectual property in synchronous and collaborative virtual space,' In: Baird, R., Lipinski, T.A. & J. J.Britz, (1999). 'Deconstructing (the concept of) intellectual property : Designing and incorporating alternative models of property ownership in the new millennium and the protection of indigenous knowledge, *Proceedings of Ethicomp* 99, 5-8.
- Ogunleye G.A. (2000), Ethics and professionalism in banking: Lessons from the recent distress in the Nigerian banking system. *NDIC Quarterly Journal*, 10,32-38.
- Ramsower, R. & Rosenbaum, S. (eds.) *Cyberethics*. Prometheus Books.
- Spinello, R. (2000). *Cyberethics: Morality and law in cyberspace*. Jones and Bartlett Publishers.
- Tavani, H. (2003). *Ethics and technology: Ethical issues in an age of information and communication technology*. Wiley.
- Tavani,H.T.(2008).Floridi'sontologicaltheoryofinformationalprivacy:Someimplication sand challenges. *EthicsandInformationTechnology*. doi:10.1007/s10676-008-9154x The Children's Online Protection Act Commission (COPA) was a commission established by Congress in the Children's Online Protection Act legislation. <http://www.Copa.commission.org>
- Tu, Chih-Hsiung (2002). The relationship between social presence and online privacy, *The Internet And Higher Education*,5, 293-318.