National Council for Higher Education

Ensuring Quality for Excellence

GUIDELINES FOR ACCEPTABLE AND RESPONSIBLE ACCESS AND USE OF DIGITAL MATERIALS IN HIGHER EDUCATION

JANUARY 2024

TABLE OF CONTENTS

Preamble 3

1. Introduction..... 4

2. Strategic use of ICT in Higher Education..... 4

2.1 Rational..... 4

2.2 Guiding framework..... 5

3. Institutional Compliance 5

4. Objectives 5

4.1. Provision of institutional controls 6

4.2 Mandatory adoption of Social media user standards and optimization..... 6

4.3 Strengthen HEI network security through user authentication..... 6

4.4 Management of BYOD Policies 7

4.5 Strengthen Institutional monitoring of acceptable use..... 7

5. INSTITUTIONAL GUIDELINES and RESPONSIBILITIES..... 7

5.1The Head of the institution..... 7

5.2The Institutional ICT Managers..... 7

5.3Management of BYOD policies..... 8

6. USERS (LEARNERS AND TEACHERS)..... 9

7. SOCIAL MEDIA AND ACCEPTABLE USE GUIDANCE..... 10

7.1The power of social media in the learning environment..... 10

7.2 Institutional access and use of Websites and Social Media guidelines.....10

7.3 Staff and Learners use of social media.....10

8. MONITORING COMPLIANCE AND EFFECTIVENESS OF THE POLICY..... 11

9. REPORTING..... 11

ANNEX1 - Sample list of the most dangerous sites by Norton (June 2023..... 12

Preamble

The National Council for Higher Education (NCHE) as the Higher Education (HE) regulator has developed guidelines to control the access and use of ICT resources in general and digital materials in particular, through informed institutional ICT *Acceptable Use Policies* (AUP) policies. The NCHE guidelines to strengthen ICT acceptable use policies are based on the relevant industry best practice in the education sector, national legal and regulatory frameworks

In the current strategic planning cycle and beyond, NCHE has positioned Information and Communication technology (ICT) as a mandatory strategic tool for regulation, teaching, learning and research. *Strategic objective 6* of the current Strategic plan 2021/22 – 2024/25 aims to "*promote the use of Information and Communication Technology in all sectors of the Council and in Higher Education Institutions*

This digital paradigm shift requires comprehensive controls to strengthen appropriate access and optimize use of ICT resources aligned with the core objectives of the Higher Education subsector.

NCHE is cognizant of the potential of Internet connectivity in the provision of access to diverse learning resources including digital material, networks, methods and tools. However, uncontrolled access to illegal and unacceptable sites can potentially cause distraction, disruption and lasting damage to a productive education environment.

Disclaimer

NCHE as the Higher education regulator reserves the right to guide compliance to a sustainable, healthy academic environment through the optimal use of scarce ICT resources. The NCHE guidelines will promote the positive utilization of the Internet education resources through improved exposure, access and use by learners and staff; while discouraging and reducing negative and defective use.

The NCHE guidelines for comprehensive Access and Use of digital materials in Higher Education are based on the minimum standard that every Higher Education institution (HEI) must have an acceptable Use policy as part of and applied in conjunction with the broader ICT policies and laws

Signed:

.....

Professor Mary J. N. Okwakol
EXECUTIVE DIRECTOR

1. Introduction

The National Council for Higher Education (NCHE) was established as the regulator of higher education under the University's and other Tertiary Institutions Act (UOTIA) 2001 (as amended). By the provisions of the ACT, NCHE is mandated to guide the establishment of institutions of higher learning and ensure delivery of quality and relevant education to all qualified persons.

2. Strategic use of ICTS in Higher Education

In the current strategic planning cycle and beyond, NCHE has positioned Information and Communication technology (ICT) as a mandatory strategic tool for regulation, teaching, learning and research. *Strategic objective 6* of the current Strategic plan 2021/22 – 2024/25 aims to "*promote the use of Information and Communication Technology in all sectors of the Council and in Higher Education Institutions.*"

NCHE has put in place strategies that respond to deliberate leveraging of ICTs for teaching and learning through the roll out and certification of Open Distance and E-learning (ODeL). In line with the National Development Plan III (NDP III), NCHE has embarked on prioritizing the accreditation of Science Technology Engineering and Mathematics (STEM) programmes to optimize the development of human capital required to support Uganda's Vision 2040. All these strategies have amplified the role of ICTs within higher education institutions.

2.1. Rationale

The digital transformation of the Higher education sector is highly dependent on the adoption of ICT resources including institutional ICT devices, systems and services but not limited to network infrastructure, Internet access, desktop computers, laptops, tablets, phones, music players or hardware, software, websites, web applications and services, and affordable the Internet access. This digital paradigm shift requires comprehensive controls to strengthen appropriate access and optimize use of ICT resources aligned with the core objectives of the Higher Education subsector.

Internet connectivity provides access to diverse learning resources including digital material, networks, methods and tools. However, uncontrolled access to illegal and unacceptable sites can potentially cause distraction, disruption and lasting damage to a productive education environment.

2.2 Guiding framework

Against this background NCHE as the Higher Education (HE) regulator is obliged to set guidelines that control the access and use of ICT resources in general and digital materials in particular, through informed institutional ICT *Acceptable Use Policies* (AUP) policies. The NCHE guidelines to strengthen ICT acceptable use policies are based on the relevant industry best practice in the education sector, national legal and regulatory frameworks. *Currently, there is no specific legislation in Uganda dealing primarily with access to digital materials and cyber security.*

However, there is a patchwork of laws that cover cyber security and the safety of information and data set by the government policy and the communications and IT regulation.

Ministry of ICT and **Uganda communication Commission (UCC)** the telecommunications regulator's and **National Technology Authority –Uganda (NITA-U** have put in place applicable guidelines are as follows :

a. **The Computer Misuse Act, 2011**('the Computer Misuse Act') is a general piece of legislation that establishes provisions for the safety and security of electronic transactions and information systems. It criminalizes the unlawful access, abuse, or misuse of computers and information systems by unauthorized persons.
b. **The Data Protection and Privacy Act, 2019('DPPA')** is an omnibus legislation that regulates data collectors, data processors, and data controllers in the collection, processing, holding or using of personal data within Uganda. The scope of the DPPA also extends outside of Uganda when the collection, processing, and controlling of personal data relates to Ugandan citizens. The DPPA also provides for measures to be taken to ensure the security of data by data collectors, processors, and controllers in respect of the data in their possession or control and the measures to be taken in the event of breaches of personal data. The DPPA further establishes provisions on the obligations of data collectors, controllers, and processors and the rights of data subjects.

3. Institutional Compliance with NCHE Guidelines for the access and use of digital materials in Higher Education

The NCHE guidelines for comprehensive Access and Use of digital materials in Higher Education are based on the minimum standard that every Higher Education institution (HEI) must have an acceptable Use policy as part of and applied in conjunction with the broader ICT policies and laws

4. Objectives

The guidelines will:

a. Inform development and review of HE Institutional ICT *Acceptable Use polices (AUP)* used in conjunction with other ICT policies, laws and network safeguards like cyber security provisions.
b. Strengthen institutional controls and responsibilities for managers, learners and staff for sustainable adoption of emerging technologies in Higher education.
c. Promoting the optimal adoption, management and use of ICT resources in HE institutions.
d. Protect users especially students in HEIs from potential negative effects of the Internet within the learning environment.

The **Acceptable Use Policy** *sets rules related to an organization's IT security policies. These include rules for accessing restricted information; changing access data, such as passwords; opening questionable email attachments; using public Wi-Fi services; and using organizational approved authentication procedures for external network users.* https://www.webwise.ie/teachers/

The AUP must include a Responsible Use Policy that treats the learners, teachers and researchers in the higher education academic space as responsible for their own ethical and appropriate use of the Internet and their devices.

The guidelines will focus on the following:

4.1. Provision of institutional controls that inhibit the availability of dangerous digital content with the following negative effects:

a. zero value to the academic environment and objectives including (non-academic content) websites for games, film, pornography,
b. Disinformation and misinformation that counters academic principles and/or harms others.
c. distortion of the positive value for high innovation potential of emerging technologies (with equally high and disruptive ability) like Artificial intelligence (AI)
d. Digital addiction- Digital addiction is a serious social, psychological, pedagogical and medical problem as consequences of a long stay on the Internet
e. Impersonation -leading to change in marks unlawful access to examinations
f. Academic fraud –attainment of fake qualifications from International degrees and diplomas Mills. .

4.2. Mandatory adoption of Social media user standards and optimization of the access and use of the education potential of new and emerging technologies.

Social media can serve as a learning tool where training videos and other materials are made easily accessible to learners in a user-friendly and engaging way. They can also be a useful tool for institutions to communicate key messages to their community and the wider public. However, the open nature of the internet means that social networking sites can leave people vulnerable if they fail to observe a few simple precautions.

HEIs must define and apply Social media Standards with appropriate use and understanding of the principles covering the use of social media in either an official or personal capacity.

4.3. Strengthen HEI network security through user authentication through a single sign on and Management of Unsafe site list and create awareness users

4.3.1 *User authentication* is a fundamental security requirement that must be included in every Institutional policy to safe guard institutional information resources and minimize external disruption.

4.3.2 M*anagement of the unsafe site lis*t through identifying, developing and or updating publicizing, institutional list of dangerous digital materials using Internet tools and ICT security information benchmarked from reputable organizations.

a. **Norton lists the top 100 dangerous websites list, (June 2023) lists** on average, about 18,000 threats with about 40 containing more than 20,000 threats; while over 50 of the websites contain hard-core pornography. (*Example Annex1*)
b. **Google** -Most major web browsers make use of the Safe Browsing API provided by Google. This tool provides a list of websites that have been detected as serving deceiving or malicious content.

4.4 Management of BYOD Policies

BYOD stands for Bring Your Own Device. This practice allows and requires users (learners and teachers) under strict security protocols to use their own personal devices to connect to the Institutional network and access "work" resources. This includes data and information that could be potentially sensitive or confidential.

Objective of the BYOD policy is to protect the security and integrity of the institutional data and technology infrastructure. It should cover acceptable use that details which activities are allowed/not allowed for institution or personal use, and which devices are permitted/not permitted.

Institutions must clearly define the BYOD policy after careful assessment of the advantages of adopting the strategy, against potential high security risks, acceptable use breaches and network management overload.

4.5 Strengthen Institutional monitoring of acceptable use and prompt enforcement.

The lines of responsibility for monitoring the different sections of the AUP and enforcement of penalties must be clearly assigned in the institutional ICT policy.

5. INSTITUTIONAL GUIDELINES and RESPONSIBILITIES

5.1 The Head of the institution is responsible for ensuring that staff and learners and managers are aware of and adhere to this policy and procedures and that breaches are managed swiftly, effectively, fairly and consistently.

5.2 The Institutional ICT Managers must effect , manage and ensure all technical security provisions for the following :

a. Passwords and login details must remain confidential
b. Users must not intentionally install software unless specifically authorized to do so
c. Users must not intentionally introduce viruses or other malicious software

d. Users must not smuggle in personal hardware to gain access to unwanted materials or vandalize institutional ICT infrastructure to compromise security .
e. The HEI's e-communications systems must not be used to Store, send or distribute messages or material which may be perceived by the recipient as:
    i. Aggressive, threatening, abusive or obscene
    ii. Sexually suggestive
    iii. Defamatory
    iv. Sexually explicit
    v. Discriminatory comments, remarks or jokes
    vi. Offensive
    vii. Bring the HEI into disrepute
    viii. Disclose sensitive information or personal data to unapproved people or organizations
    ix. Intentionally access or download material containing sexual, discriminatory, offensive or illegal material
    x. Originate or participate in email chain letters or similar types of communication
    xi. Harass or bully another person
    xii. Create material with the intent to defraud

Any attempt by a user to compromise the security or functionality of the institutional networks and its ICT systems, either internally or externally, should be considered as "hacking".

f. Monitoring the different sections of the AUP and enforcement of penalties as assigned in the institutional ICT policy.
c. Define, generate, publicize and update institutional Blocked categories list of dangerous digital materials using Internet tools benchmarked from best practice

5.3 Management of BYOD policies

The Bring Your Owen Device (BYOD) strategy is widely accepted in higher education to counter the shortage of end–user devices for teaching and learnnig in institutions and to increase productivity by maximizing out of the class learning .BYOD also presents high risk of smuggled access and dissemination of illegal and unacceptable material, the security risks and network support for diverse types of devices network overload and high student distraction.

i. The adoption of BYOD by institutions must be carefully weighed against the resources to mitigate challenges.
ii. The most commonly accepted BYOD policies range from enabling remote tools on personal mobile phones to requiring users to provide their own laptop or computer.
iii. Clearly define Institutional BYOD security policies and include them in the acceptable use. This should include best practices for creating strong passwords, limitations on downloading and installing apps, and what to do in the event of a security breach. and

two-factor authentication policies, protocols for backing up sensitive information, and procedures to be followed if a device is lost or stolen

6. USERS – (LEARNERS AND TEACHERS)

a. Must not bring into the HEI environs any material that would be considered inappropriate. This includes files stored on memory sticks, CD, DVD or any other electronic storage medium, or accessing information via the HEI Wi-Fi, which would be viewed as inappropriate.

b. Are responsible for all files that are stored in their storage area and any visits to websites by their user account. Users must not breach the copyright of any materials whilst using the HEI's ICT systems.

c. must ensure that:

   i. They keep personal data safe, taking steps to minimize the risk of loss or misuse of data

   ii. Personally identifiable and sensitive, confidential data is protected with the use of passwords, locking of computers, logging off shared devices, use of encryptions where appropriate and increasing the use of remote access rather than transporting or transferring information

   iii. Personally identifiable, sensitive and confidential data must not be stored on any form of removable media (e.g. memory sticks, external hard-drives, surfaces or laptops, and CDs or DVDs) and it must not be stored on users' personal devices (e.g. home PCs, mobile 'phones)

   iv. When using mobile devices (e.g. surfaces and laptops) users encrypt/password protect documents; password protect the device; ensure the device has appropriate virus and malware checking software

   v. Users must not carry out any of the following deliberate activities:

      - corrupting or destroying other users' data
      - violating the privacy of other users
      - disrupting the work of others
      - denying service to other users (for example, by deliberate or reckless overloading the network)
      - other misuse of the HEI's ICT and networked resources, such as the introduction of viruses or other harmful software to the HEI's ICT systems
      - unauthorized monitoring of data or traffic on the HEI's ICT network or systems without the express authorization of the owner of the network or systems

6.1 Management of unsafe websites

Users must report to their line manager or the IT Department access to inappropriate or illegal material including:

a. Requests to unblock a website and do not attempt to bypass Institutional network web filters.
b. Any access to a site that should be blocked by web filters to their line supervisor and contact the relevant ICT technical support team with a request to block a website.
c. Users must only access appropriate content availed on the institutional network and not intentionally visit sites or news groups that are obscene, indecent or advocate illegal activity, as described in the Blocked categories list.

7. SOCIAL MEDIA AND ACCEPTABLE USE GUIDANCE

7.1 The power of social media in the learning environment

a. Social media is now formally recognized as a tool that Staff and learners may be required to use social media for their work, and therefore institutional guidance includes activities undertaken for work and personal purposes. This guidance applies to all social networking sites, chat rooms, forums, podcasts, blogs, texting, online encyclopedias with open access (such as Wikipedia) and content sharing sites such as YouTube.

b. Social media can serve as a learning tool where training videos and other materials are made easily accessible to learners in a user-friendly and engaging way. They can also be a useful tool for schools to communicate key messages to their community and the wider public. However, the open nature of the internet means that social networking sites can leave people vulnerable if they fail to observe a few simple precautions.

7.2 Institutional access and use of Websites and Social Media guidelines:

a. HEIs must i) define and apply Social media Standards with appropriate use and understanding of the principles covering the use of social media in either their official or personal capacity. ii) Implement and enforce compliance with the Social Media Policy and awareness of applicable Institutional AUP guidelines.
b. Only use approved Institutional social media accounts for official business and where appropriate, use institutional branding and a professional image or persona on such account.
c. Provide access to appropriate content, tools and other educational resources from the Internet and prohibit intentional visit to sites that are obscene, indecent or advocate illegal activity.
d. Identify and publicize education sites lists for different education and research purposes

7.3 Staff and Learners use of social media

Users:

a. are responsible for the content they post and penalties will be applied to individual users if policies are breached1
b. must be aware that their social media content/footprint may being the public domain available for anyone to see, indexed by Google and archived for posterity.
c. should keep their passwords confidential, should change them often and should at all times be vigilant about what may or may not legitimately be posted online, and should be aware that it is not safe to reveal home addresses, telephone numbers or other personal information online.
d. are encouraged to be mindful of the risk of fraud and identity theft online and are advised to carefully consider the amount of personal information they display, share or reveal online. Staff and learners should always keep their passwords secret and take all necessary measures to protect access to accounts.

8. MONITORING COMPLIANCE WITH AND EFFECTIVENESS OF THE POLICY

Effectiveness and compliance of this policy should be regularly monitored by the Higher Education Institution's Director of ICT or such a person with overall responsibility for ICT in the institution.

9. REPORTING

Higher Education Institutions - will be required to send regular reports to the NCHE about their Acceptable Use Policy (AUP) implementation and management as required for ICT compliance. Compliance with these guidelines will be monitored by NCHE as incorporated into and implemented under the Institutional ICT policy.

ANNEX 1

Sample list of the most dangerous sites by Norton (June 2023)

Norton is one of the most popular antivirus software that is available on the market. It's a comprehensive suite of security tools that provides protection from all sorts of threats including viruses, malware and spyware.

- Ucoz. com
- 17ebook. co
- sapo .pt
- aladel. net
- bpwhamburgorchardpark. org
- clicnews. com
- Amazonaws .com
- dfwdiesel. net
- divineenterprises. net
- fantasticfilms. ru
- Blogspot .de
- gardensrestaurantandcatering. com
- ginedis. com
- gncr. org
- hdvideoforums. org
- hihanin. com
- kingfamilyphotoalbum. com
- 4shared .com
- likaraoke. com
- mactep. org
- magic4you. Nu
- sendspace .com
- marbling.pe. kr
- nacjalneg. info
- pronline. ru
- purplehoodie. com
- qsng. cn
- comcast .net
- seksburada. net
- sportsmansclub. net
- stock888. cn
- fc2 .com
- tathli. com
- teamclouds. com
- texaswhitetailfever. com
- Hotfile .com
- wadefamilytree. org
- xnescat. info
- Mail. Ru
- yt118. com