

NJA College of Education, WA



ACCEPTABLE USE POLICY

Purpose/Objectives

To educate staff, students and our wider community on acceptable standards in using the College's ICT resources effectively as a tool for learning and to support and develop lifelong learning. This Acceptable Use Policy also sets out the responsibilities and required behaviour of users of the College's information systems, networks and computers.

The purpose of the ICT Policy is

- i. To provide optimum security for the use of the College's Information System, networks and computers.
- ii. To provide the resources and expertise that will allow users of ICT resources in the College to be discriminating and discerning in the selection and use of a range of Information and Communication Technology resources.
- iii. To develop a broad and balanced experience of the range of information and communication systems and their applications and an understanding of their capabilities and limitations within our College.

8.2. Scope/Application

All members of the College staff who have been granted access to use the facilities together with any others, including students, who may be granted permission to use the College's information and communication technology facilities by the Head of ICT Services are subject to this policy.

8.3. The Policy Statement

8.3.1. User identification and authentication

Each member will be assigned an associated account password which must not be divulged to anyone, including ICT support services staff, for any reason. The College password should not be used as a password for any other service. Individual members are expected to remember their passwords and to change it if there is any suspicion that it may have been compromised.

Each member of staff will also be assigned a unique email address for his or her individual use. Members must not use the College email address assigned to anyone else without their explicit permission.

Email addresses are College-owned assets and any use of these email addresses is subject to College policies.

In order to encourage gender sensitivity in participation, NUJACED would consciously eliminate any form of barrier that limits women from taking full advantage of the opportunities offered by ICT unit. The College will put on our website issues on gender equity on the acceptable use of ICT for students and staff to share their views.

8.3.2. Personal use of facilities

College information and communication facilities, including email addresses and computers, are provided for academic and administrative purposes related to work or study at the College.

Occasional personal use is permitted but only as long as:

- It does not interfere with the member of staff's work.
- It does not contravene any College policies.
- It is not excessive in its use of resources.

College facilities should not be used for the storage of data unrelated to membership of the College. In particular, College facilities should not be used to store copies of personal photographs, music collections or personal emails.

Members of staff should not use a personal (non-College provided) email account to conduct College business and should maintain a separate personal email account for personal email correspondence.

All use of College information and communication facilities, including any personal use, is subject to College policies.

8.3.3. Connecting devices to College networks

In order to reduce risks of malware infection and propagation, risks of network disruption and to ensure compliance with other policies it is not permitted to connect personally owned equipment to any network socket which has not been provided specifically for the purpose. It is permissible to connect personally owned equipment to the College's wireless networks.

To further reduce risks of data loss, members of staff should not connect any personally owned peripheral device which is capable of storing data (for example a personally owned USB stick) to any College-owned equipment, irrespective of where the equipment is located.

Any device connected to the College network must be managed effectively.

8.3.4. Software

All software loaded on the networks or on computer systems belonging to the College must be properly licensed by the manufacturer and its use must conform to the terms of such licences. The following guidelines must be adhered to:

- Members of staff must not install onto College computers software for which the necessary licences have not been acquired
- Care must be taken when making any copy of such software, or when enabling its use by more than one person, that the terms of any licences have not been breached.
- Software and other material downloaded and installed from the Internet must be licensed appropriately. The use of shareware software is always subject to a licence agreement, and acceptance of the terms of such a licence is implied when software is downloaded.
- The College does not condone the unlicensed copying or use of software on computers belonging to members of staff, and the liability for the infringement of copyright in such cases is likely to rest with the individual concerned.

The College has the right to audit, by electronic and other means, the use of copyright software on any computer system belonging to the College. Any breach of these guidelines may result in disciplinary action.

8.3.5. Use of services provided by third parties

Wherever possible members should only use services provided or endorsed by the College for conducting College business. The College recognises however that there are occasions when it is

unable to meet the legitimate requirements of its staff and students and that in these circumstances it may be permissible to use services provided by other third parties.

8.3.6. Unattended equipment

Computers and other equipment used to access College facilities must not be left unattended or unlocked if logged in. Staff must ensure that their computers are locked before being left unattended. Care should be taken to ensure that no restricted information is left on display on the computer when it is left unattended.

Particular care should be taken to ensure the physical security of all equipment when in transit.

8.3.7. Unacceptable use

In addition to what is already written above, the following are also considered to be unacceptable uses of College facilities

- i. Any illegal activity or activity which breaches any College policy.
- ii. Any attempt to undermine the security of the College's facilities.
- iii. Providing access to facilities or information to those who are not entitled to access.
- iv. Any irresponsible or reckless handling or unauthorised use of College data.
- v. Any use which brings the College into disrepute.
- vi. Any use of College facilities to bully, harass, intimidate or otherwise cause alarm or distress to others.
- vii. Sending unsolicited or unauthorised bulk email (spam) which is unrelated to the legitimate business of the College.
- viii. Creating, storing or transmitting any material which infringes copyright.
- ix. Creating, storing or transmitting defamatory or obscene material.
- x. Watching movies, chatting on the internet during working hours.
- xi. Watching, downloading or uploading pornographic files.
- xii. Using software which is only licensed for limited purposes for any other purpose or otherwise breaching software licensing agreements.
- xiii. Failing to comply with a request from an authorised person to desist from any activity which has been deemed detrimental to the operation of the College's facilities.

- xiv. Failing to report any breach or suspected breach of information security to ICT support services.
- xv. Failing to comply with a request from an authorised person for you to change your password.

8.4. Supporting Procedures

Minor breaches of policy will be dealt with by ICT Support Services. Heads of Department may be informed of the fact that a breach of policy has taken place.

More serious breaches of policy (or repeated minor breaches) will be dealt with under the College's disciplinary procedures.

Where appropriate, breaches of the law will be reported to the police. Where the breach has occurred in the jurisdiction outside Ghana, the breach may be reported to the relevant authorities within that jurisdiction.

8.5. Gender-responsive/Inclusion statement(s)

To provide the resources and expertise that will allow both genders to use ICT resources in the College. And also for them to be discriminating and discerning in their selection and use of varied ranges of Information and Communication Technology resources.

8.6. Responsibility for Implementation

All employees of the College at all levels and roles are responsible for the implementation of this policy.

It is the responsibility of the Vice-Principal and Head of ICT to ensure review of the policy. It is the responsibility of all to engage positively in that review and ensure implementation.

8.7. Responsibility for Monitoring, Implementation and Compliance

The following officers shall be responsible for the monitoring and ensuring compliance with the conditions set out in this policy document.

- The Principal
- Head of ICT
- College Secretary

8.8. Status

Upon receipt of Computers, Academic Board took a decision to have a policy in place to ensure equitable use of the ICT resources in the College.

8.9. Key Stakeholders

- Students
- Staff
- Relatives of Staff
- Alumni
- Visitors to the College
- All persons working on behalf of the College

8.10. Approval Body

- College Council

8.11. Initiating Body

Academic Board

8.12. Definition of Terms

8.12.1. ICT – Information and Communication Technologies

8.12.2. Computer – PC's, Mobile Phones, Tablets, Video Camera etc.

8.12.3. Software – The programmes and other operating information used by the computer.

8.12.4. Information Security – The practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording, or destruction

8.12.5. USB Stick – Universal Serial Bus - Flash Drives

8.12.6. Network – A telecommunications network which allows computers to exchange data

8.12.7. Internet – Network of Networks

8.12.8. Email – Messages distributed by electronic means from one computer user to one or more recipients via a network.

8.13. Related Legislation

- National ICT Policy, Ghana
- NUJACED College Handbook

8.14. Related Policy and Other Documents (Exhibits)

- National ICT Policy, Ghana
- NUJACED College Handbook
- Copyrights regulations, The 1992 Republican Constitution of Ghana

8.15. Effective Date

- September 17, 2020

8.16. Review Date

- September 17, 2022

8.17. Key Words

- ICT, Computer, Software, Information Security, Network, Internet, Email.

8.18. Owner/Sponsor

- College Principal
- Head - ICT Unit

8.19. Author

- Governing Council

8.20. Further Information

Nusrat Jahan Ahmadiyya College of Education,

P.O.Box 71, Wa

Upper West Region.