



University of Ghana

Acceptable Use Policy

1. Overview

UGCS is committed to protecting members of the University of Ghana community, including employees, students and affiliated members, from damaging or illegal actions perpetrated knowingly or unknowingly. Users are encouraged to use the IT resources in line with the mission of the university to further the goals and objectives of their work, study or research.

2. Purpose

The Acceptable Use Policy seeks to outline the acceptable use of information technology resources within University of Ghana and to inform the University's staff, students, and other individuals entitled to use University of Ghana ICT facilities, of the regulations relating to the use of information and communications technology systems. Inappropriate use of these systems exposes University of Ghana to legal system compromise and viral risks

3. Scope:

This policy applies to:

- All University of Ghana students, staff, faculty and others granted use of University of Ghana's information resources,
- All computing and data communications equipment owned, leased or operated by University of Ghana,
- All equipment connected to the University's data network, regardless of ownership, and
- All individuals who use equipment connected to the University's data network, regardless of their affiliation with the University.

4. The Policy

4.1 General Use & Ownership

1. All users shall comply with existing University policies.
2. Users will not access, interfere with or remove any ICT facility, data or information unless they have been authorized to do so.
3. Users shall use ICT facilities in a manner that is consistent with their role.
4. All use of ICT facilities shall be lawful, honest and decent and with due regard for the rights and sensibilities of other people.
5. Users are individually responsible for appropriate use of all resources assigned to them, including the computer, the network address or port, software and hardware. Therefore, users are accountable to the University for all use of such resources. Authorized users of University of Ghana resources may not allow unauthorized users to access the network by connecting any device to the University of Ghana network.

4.2 Security Information

1. Users will not use ICT facilities in such a way as to deliberately disrupt or interfere with the use of such facilities.
2. All software on any equipment connected to University ICT facilities shall be properly licensed and the terms of the license strictly observed.
3. Users shall not deliberately create, use or distribute materials that could bring the University into disrepute.
4. Authorized administrators of the University may access or monitor electronic data held on or transiting University ICT facilities where there is a belief that the user may be in breach of University regulations or the law, or where required to do so by an external law enforcement agency, e.g., the Police, or where users are absent and no arrangements have been made to allow access to information crucial to the working of the University.
5. Users should make a reasonable effort to protect their passwords and to secure resources against unauthorized use or access.

4.3 Unacceptable Use

The list below is by no means exhaustive, but attempts to provide a framework for activities, which fall into the category of unacceptable use.

1. Under no circumstances is a user of University of Ghana authorized to engage in any activity that is illegal under local and international law while utilizing the university's IT resources.
2. Users must not volunteer their account passwords to others or allow the use of their accounts by others including family and other household members.
3. Users must not breach security or disrupt network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless such activities are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, unauthorized placing of information technology resources on and

removal from the university's network, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

4. Port scanning or security scanning is expressly prohibited unless prior notification is given to University of Ghana Computing Systems.
5. Executing any form of network monitoring which will intercept data not intended for the employee's device is prohibited, unless this activity is a part of the employee's normal duty.
6. Users must not circumvent the authentication or security mechanisms of any device, network or account controlled by the University.
7. It is prohibited for users to send unsolicited email messages, including "junk mail" or other advertising material, to individuals who did not specifically request such material (email spam).
8. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type is prohibited
9. Users must refrain from connecting network devices unto the UG network without authorization.
10. Usurping the university's bandwidth for commercial purposes or personal interest is prohibited.

5. Consequences of Misuse of Computing or Network Privileges

Members of the university community found to have violated this policy may be subject to disciplinary action by University of Ghana authorities including dismissal from the university.

5.1 Cooperation Expected

Members of the university community, when requested, are expected to cooperate with system or network administrators in any investigation of system abuse. Failure to cooperate may be grounds for suspension or cancellation of access privileges, or other disciplinary actions.

Members of the university community who feel they have been victims of abuse should contact the University of Ghana Computing Systems.

6. Definitions

- The term "User" refers to any person authorized to use University ICT facilities.
- ICT facilities are defined to be computing equipment, communications equipment and software applications provided to support the learning, teaching, research, enterprise and administration activities of the University of Ghana.
- Chain letters are letters that promises some form of reward when forwarded to a number of users
- Ponzi schemes are fraudulent investment operation
- Pyramid scheme is a model that promises payments based on an individual enrolling others.

7. Ownership

The university council owns this policy. The CITO of University of Ghana Computing Systems has direct responsibility for maintaining this policy and providing guidance and advice on its implementation.

8.0 Revision History

Version	Date	Change Description	Author
0.1	Feb 2014	Initial draft for review	Mawuli Takpo
0.2	22 nd May 2014	Review by all departmental Heads and final update by Head, IT Planning, Security & Support	Benjamin Cobblah
0.3	2 nd June 2014	Review by Deputy CITO, IT Planning, Security and Support	Frederich Kwakye-Mafo
1.0		Final draft – Review by CITO, UGCS	Lucas Y. Chigabatia
1.1	March 2016	Reviewed by English & IT Planning Unit Team	Benjamin Cobblah

DRAFT