UNIVERSITY OF EDUCATION, WINNEBA
POLICY FOR RESPONSIBLE USE OF UNIVERSITY INFORMATION TECHNOLOGY RESOURCES

1.0 INTRODUCTION

Information Technology (IT) resources at the University of Education, Winneba (UEW) are intended primarily to serve the teaching, research and administrative purposes of the University. The University is therefore responsible for ensuring that resources and facilities it has provided are in fact used for the purposes for which they were intended.

The University grants members of the University community shared access to these resources in support of accomplishing its mission. Access to University IT facilities and services is a privilege and not a right. This privilege is extended to all faculty, staff and students and may be limited or revoked if the user violates University policies or national laws. All users of these resources are therefore required to use them in an effective, efficient, and responsible manner.

1.1 Purpose

The purpose of this Responsible User Policy is to ensure that the University's IT resources are used responsibly, effectively and efficiently to promote the basic mission of the University in teaching, research, administration and service. In particular, this policy aims to achieve the following specific objectives:

- To ensure the integrity, reliability, availability and good performance of IT resources.
- To ensure that use of IT resources is consistent with the principles and values that govern use of other University facilities and services.
- To ensure that IT resources are used for their intended purposes.

1.2 Scope

This policy applies to all IT resources and all users, including but not limited to University faculty, staff and students. The policy also applies to the use of privately owned computers connected to the University network.

2.0. GENERAL PRINCIPLES

Access to modern IT is essential to UEW's mission of providing students with educational services of the highest quality. The pursuit and achievement of the mission of education, research and community service require that the privilege of using IT resources be made available to the entire university community. The preservation of that privilege for the full community requires that each faculty member, staff, student and any other user comply with institutional and external policies for appropriate use. To assist and ensure such compliance, UEW establishes the following policy:

i. Use of UEW's IT resources shall be consistent with the education, research and community service mission of the University, all national regulations and this policy document.
ii. Each user of IT services bears primary responsibility for his or her use of these services and for the information he or she transmits, receives or stores through use of these services.
iii. Incidental use of IT services for personal use is acceptable but is limited to such responsible activity as minimises disruption of University business.
iv. Connection of privately owned computer equipment to University IT services is permitted. Access to University IT services from these computers is also permitted. All such usage is governed by this policy.
v. Information technology provides an important means for both public and private communication. Users and network administrators will respect the privacy of person-to-person communications in all forms including telephone, electronic mail and file transfers.
vi. In the normal course of system maintenance, both preventive and troubleshooting, staff members operating the computer systems may be required to view files. Staff is required to maintain the confidentiality and

privacy of information in such files unless otherwise required by law or University policy.

vii. This policy may be supplemented with additional guidelines by units that operate their own computers or networks, e.g., the University Library.

3.0. USER RIGHTS AND RESPONSIBILITIES

3.1 User Access

Access to information technology resources is granted by the University solely for the Individual's own use. Users are responsible for maintaining the security of their own accounts and passwords for access to IT resources. Sharing access with another individual undermines the security of an account, leaving it vulnerable to abuse by others. Accounts and passwords are normally assigned to individual users and are not to be shared with any other person without authorisation by the network administrator. Users are responsible for any activity carried out under their accounts. Users should not maintain the default password given them by the Network Administrator. No user is to use an account with administrative privileges.

3.2 User Privacy, Integrity and Operational Security

The privacy of all users and the integrity and operational security of the University's information technology system must be respected by all. Each user must respect the privacy and integrity of other computer users. No user should view, copy, alter or destroy another's personal electronic files without permission. The fact that an individual account and its data may be unprotected does not confer any right to access it without permission.

Users should also be aware that their use of University IT resources is not completely private. While the university does not routinely monitor individual usage of its IT resources, the normal operation and maintenance of these resources require the backup and caching of data and communications, the logging of activity, the monitoring of general usage patterns and other such activities that are necessary for the provision of service. The University may also specifically monitor the activity and accounts of individual users of University IT resources, including individual login sessions and the content of individual communications, without notice, when:

i. It reasonably appears necessary to do so to protect the integrity, security, or functionality of university IT resources or to protect the university from liability; and
ii. There is reasonable cause to believe that the user has violated or is violating this policy.

3.3 Misuse of IT Resources

Users must not use University IT resources in the commission of any illegal or otherwise unauthorised act.

Examples of activities that may violate this provision, include, but are not limited to the following:

- Unauthorized upload, download, or other digital reproduction of copyrighted materials, including software, music and films.
- Unauthorized storage of copyrighted materials, including software, music and films, on University owned or controlled IT resources.
- Use of University IT resources for the viewing, accessing, or transmitting of offensive material is strictly forbidden. This applies to any screen display or printing of images, sounds or messages that could reasonably be considered obscene, pornographic, profane or otherwise objectionable.
- Use of University IT resources to threaten, harass, defame, libel or slander any other person.
- Unauthorized interception of electronically transmitted information.
- Extensive recreational game playing, especially during normal working hours.

3.4 Unauthorized Commercial Use

Users must not use University IT resources for any unauthorised commercial purposes. Use of any University IT resources for personal gain or profit is prohibited.

The University's IT resources are provided in support of the University's educational, research and service missions; therefore, uses that are consistent with this purpose must always receive the highest priority. Other uses, such as those that indirectly support this mission, including reasonable and limited personal use, while permissible, must necessarily receive a lower priority. Unauthorised commercial use

of University IT resources is inappropriate and inconsistent with the University's mission.

Examples of activities that may violate this provision, include, but are not limited to the following:

- Using University hosted IT services to advertise, provide services to, and/or sell commercial products or services
- Using University IT resources to distribute unsolicited advertisements on behalf of commercial entities

3.5 Data Security and Confidentiality

Data originated or stored on University IT equipment is University property. Users are responsible for ensuring the confidentiality and appropriate use of institutional data to which they are given access. Users must not access or attempt to access data on any University system they are not authorised to access. They must not make or attempt to make any deliberate and unauthorized changes to data on the University system. If a user finds that he has access to data he believes he is not authorised to view, he will exit from that data and report the problem to the Network Administrator.

3.6 Internet and Email

Use of the Internet and email by faculty, staff and students is permitted and encouraged where such use is consistent with the University's mission. Occasional personal use of email and the Internet is acceptable. However, use of the University of Education, Winneba domain name to conduct business other than official University business is prohibited.

Users are permitted to engage in the following activities:

i. During working hours, access information for the performance of their job.
ii. During working hours, participate in news groups, chat sessions, and email discussion groups, provided these sessions have a direct relationship to the user's job with the University.

iii. During personal time, retrieve non job-related information to develop or enhance the user's knowledge and skill in information retrieval.

3.7 Use of Internet Bandwidth Resources

The University is committed to pursuing an efficient and fair network usage policy in order to meet the growing bandwidth requirements of the entire University. The aim of this policy is to manage bandwidth use to avoid degradation and ensure network efficacy. Management of Bandwidth resources shall be entrusted to the University Network Administrator. Bandwidth usage shall be subject to the following:

i. Internet Bandwidth will not be over utilised as to prevent access to critical information, research and online educational projects. Bandwidth allocation shall be made in the following order:

    a. Online Distance Education
    b. Research
    c. E-mail

ii. Personal and non educational online materials are not allowed through the University's Internet infrastructure.

iii. Unauthorised persons are not allowed to access internet facilities within the University network.

iv. Network devices shall be monitored for optimal functionality to ensure constant accessibility to Internet Bandwidth.

4.0 SANCTIONS

Heads of Department/Section/Unit, the Registrar, the University Disciplinary Committee and the Network Administrator will monitor and apply certain penalties to non compliant users as follows:

- The Network Administrator is empowered to suspend any account to protect the integrity, security, functionality of the University's IT resources or data in consultation with the Coordinator of ICT. The Coordinator will duly advise the account holder and the division or department head of such an action. If such an action is the result of repeated non-compliance of any portion of this policy, then the Coordinator will inform the Registrar of the University who may pursue further disciplinary measures against the non-compliant.

- Heads of Department/Section/Unit are empowered to monitor non-compliant usage of the University's IT resources as described in his policy. Heads are empowered to seek immediate suspension of accounts of non-compliant users from either the ICT Coordinator or Network Administrator. Heads may, at their discretion, refer non-compliant user to the Registrar who may pursue further disciplinary actions.

Restoration of any suspended account(s) shall be effected by ICT Coordinator/Network Administrator after an application of "Request for Restoration of Account" has been made by the user through the division/department/section head to the Coordinator of ICT.

5.0 DEFINITIONS

Access: Ability given to individual or groups of users to use information stored on or via University resources. This includes but is not limited to the ability to read, write, view, create, alter, store, retrieve and disseminate information.

Account: The combination of user name and password assigned to a user for access to information technology resources.

Authorized Use: Any use consistent with the education, research and service mission of the University.

Commercial Use: An activity conducted for commercial/private profit. This includes but is not limited to soliciting sales or funds, marketing or advertising a product or service, posting an advertisement to a newsgroup and reselling University resources. University authorized commercial activities are exempted.

Email: Electronic method of sending and receiving messages from and to electronic addresses associated with specific owners.

Information Technology (IT): Application of modern electronic and computing capabilities to the creation and storage of meaningful and useful facts or data and to its transmission to users by various electronic means.

Information Technology Resources: Information Technology Resources referred to in this policy includes any information in electronic format or any hardware or software that makes possible the transmission, storage or use of such information. Included in this definition are electronic mail, databases, digitized information, personal computers, workstations, servers, operational software, network devices and interfaces, electronic storage, messaging, communications devices and other peripherals.

Institutional Data: Information about individuals and the University that is recorded, maintained, administered and retained by the University, e.g. information in student records and employee files and financial data.

Internet: The global interconnection of data networks or bulletin board systems that commonly use (but are not limited to) the Internet Protocol.

Network Administrator: A person who has system privileges, and is responsible for the operation and security of the University IT resources. Network administrators oversee the day-to-day operation of the system and are authorised to determine who is permitted access to particular IT resources in accordance with existing policies and procedures.

Normal Working Hours: Monday to Fridays from 8:00 a.m. to 5:00 p.m. This does not include approved rest break periods.

University: The term "University" means the University of Education, Winneba and includes all its campuses and constituent parts.

User: All persons (including faculty, staff, students and any other person) authorised to access and/or use University IT resources.