BIU

EDUCATION FOR LIFE LEADERSHIP

BLANTYRE INTERNATIONAL UNIVERSITY

ICT ACCEPTABLE USE POLICY

January 2017

Private Bag 98, Blantyre, Malawi
Tel: +265 1 831516 | Fax: +265 1 831514
Email: info@biu.ac.mw
Website: www.biu.ac.mw

Contents

Preamble

Information is the lifeblood of every organization. The effective creation, organization, access, and security of information are crucial to achieving the goals of an organization.

This document summarizes the minimum expectations for the usage of BIU's Information and Communications Technology (ICT) resources, which include information and infrastructure.

Purpose

The ICT Acceptable Use Policy is intended to inform University staff, students, and authorized individuals about the regulations governing the use of Information Communications Technology systems within the University.

The term "User" refers to any person authorized to use the University's ICT facilities.

ICT facilities encompass computing equipment, communication equipment, and software applications provided to support the University's learning, teaching, research, enterprise, and administrative activities.

It is imperative that all users exercise due care in their use of ICT facilities. Users must ensure that these facilities are employed in an appropriate manner and in a way that does not jeopardize the ability of themselves or others to use the resources.

The Policy

The University expects all individuals to exercise caution and responsibility in their use of ICT facilities, whether directly (University facilities) or indirectly (third-party equipment connected to University facilities).

Users must comply with all existing University policies.

All software on equipment connected to University ICT facilities must be properly licensed, and the terms of the license must be strictly adhered to.

Users are not allowed to access, interfere with, or remove any ICT facility, data, or information from any room or University premises unless they have explicit authorization to do so.

Users should use ICT facilities in a manner consistent with their roles.

Deliberate disruption or interference with the use of ICT facilities by others is prohibited.

All use of ICT facilities must be lawful, honest, and respectful of the rights and sensitivities of others.

Users must not create, use, or distribute materials that could bring the University into disrepute deliberately.

University officers may access or monitor electronic data held on or transiting University ICT facilities if there is a belief that an individual may be in breach of University regulations or the law, or when required by external agencies such as the Police, or in cases where individuals are absent, and no arrangements have been made for access to critical information necessary for the University's operation.

Individuals in violation of this policy are subject to disciplinary procedures initiated by the Registrar, Head/Dean, or relevant authorities responsible for the person concerned.

Ownership

The ICT Officer, in consultation with the Office of the Registrar, is responsible for maintaining this policy and providing guidance on its implementation.

A. Appendix: Guidance on the Application of the ICT Acceptable Use Policy

The appendix provides specific examples of how the policy applies and offers additional guidance and best practices.

A.1 Details on acceptable use in specific areas may be found on the University's intranet.

A.2 The University acknowledges that, as an academic institution, there may be legitimate reasons for some staff and students to access, download, or store electronic information that could be considered offensive or unacceptable (e.g., explicit or violent content). In such cases, individuals must obtain written approval from their Head of Department or Dean before engaging in such activities and must comply with any conditions set by the Dean, Director, or VCE member.

A.3 Users who connect personal equipment to University ICT facilities do so at their own risk. The University is not responsible for any consequential damage, virus infection, corruption, or loss. The Network Connection policy outlines the regulations for connecting devices to the network.

A.4 Staff with legitimate access to personal data must only access such data to the extent they have been specifically authorized by the University or as part of their role.

A.5 Dos and Don'ts

Do:

✓ Report any security breaches of University ICT facilities to IT support personnel.

✓ Ensure that personal ICT equipment has adequate virus and firewall protection. The University may refuse connection to devices that are not adequately protected.

✓ Protect University IT equipment on loan or used outside of the University from improper use. University laptops should not be used by friends or relatives.

✓ Manage your file store and mailbox to stay within resource allocations. A full mailbox may prevent communication and file storage.

✓ Exercise caution when sending emails to ensure they do not contain content that could be considered discriminatory or offensive.

✓ Be mindful when using your University email address to prevent personal opinions from being misconstrued as the University’s stance.

Don’t:

✗ Attempt to impersonate the identity of others or send emails with misrepresented originator or recipient addresses.

✗ Share your password with others or use someone else’s User-ID and password.

✗ Leave a logged-in computer unattended.

✗ Connect personal ICT equipment to University facilities that do not comply with the network connection policy.

✗ Make, transmit, or store an electronic copy of copyright material without the owner’s permission.

✗ Send unsolicited bulk emails, also known as SPAM, either within or outside the University.

A.6 Legal Frameworks.

The following legal frameworks apply:

Computer Misuse Act 1990,

Data Protection Act 1998,

Defamation Act 1996,

Copyright, Designs and Patents Act 1988,

Freedom of Information Act 2000,

the Communications Act 2003, and the Human Rights Act 1998.