University of Gloucestershire
Library, Technology & Information Service

Network & Wireless Policy

LTIU-POL-05

Document Control

Issue/Amendment Record

Issue	Date of Issue	Reason for Issue
1	00/00/00	Major Revision

Document Ownership

	Name and Title	Signature	Date
Author	**Robin Livesey** Content Support & Information Manager		
LTI Approval	**Nick Moore** Director LTI Service		
University Approval	**David James** Dean of Academic Development		
Release Authority	**Robin Livesey** Content Support & Information Manager		

Introduction

The University of Gloucestershire (the "**University**") is committed to providing a safe and secure environment, where students, staff, visitors and contractors can use technology to support their study/work and development, whilst being free from harassment, bullying or discrimination.

The following policy has been developed to help foster and promote a suitable and secure learning/working environment. Therefore, all students, staff, visitors and contractors are required to follow the rules stated in this policy when using the University's IT systems, network, WiFi, email and/or internet facilities.

The University will enforce this policy in order to protect those in its care, on its property or using its IT Services.

The University's Library, Technology and Information Service ("**LTI**") policies, including this policy, may be amended from time to time as deemed appropriate. Please check back frequently to see any updates or changes to this policy.

Everyone who accesses the University's IT systems, network, WiFi, email and/or internet facilities must familiarise themselves with the contents of this policy.

Type of Policy

User Policy

Purpose

The purpose of this Network & Wireless Policy is to establish the rules which govern the use of the University's network/wireless network, and how those rules apply to all students, staff, visitors and contractors.

These rules are necessary to preserve the integrity, availability, and security of systems and data belonging to the University, as well as the general safety of students, staff, visitors and contractors of the University. The policy clearly articulates what is expected of all system users, along with the potential consequences of failing to adhere to the rules.

Scope

The rules set out in this policy apply to anyone using the University's network/wireless network, whether on campus or off campus. Unless specifically authorised in writing by the Director of the LTI Service, there are no exceptions to this policy. The Director of the LTI Service can be contacted via the IT And Library Helpdesk.

Please note that this policy also applies where you access the University's network through your own device.

Rules of use

All Users Will

- have read, understood, and accepted full responsibility for adhering to this policy and its terms and conditions
- be aware that violation, or attempted violation, of this policy may lead to their temporary or permanent exclusion from the University systems and services, including exclusion of access from the University's network, WiFi, email and/or internet facilities
- comply with the University's instructions in relation to the usage of the University's network/wireless network as issued from time to time
- act responsibly, and ensure that the network is being used lawfully, ethically and courteously
- be aware that, due to the risk of 'hacking', the university cannot guarantee the privacy of network traffic
- respect the rights of other users, the integrity of the systems and related physical resources
- respect all computer software copyrights and adhere to the terms and conditions of any licence to which the university is a party

All Users Will Not

- introduce, launch, install or attach any unauthorised equipment to the university network, except allowed devices in halls of residence
- use the University's network to transfer any information that contains illegal content (eg child pornography, sectarian propaganda designed to incite violent acts)
- 'proxy' or share connections, making them available to other users
- launch or facilitate network attacks (eg Distributed Denial of Service, DDoS)
- scan the network for devices (this is to stop unscrupulous individuals finding, and taking advantage of, any vulnerabilities within the University's network)
- run interfering network services (eg Dynamic Host Configuration Protocol, DHCP - Domain Name Service, DNS)
- circumvent firewall or internet security protections

The Library, Technology and Information Service reserve the right to disconnect any device from the University's network, if it is believed that the device poses a risk to security.

Consequences of breaching this policy

Any attempt to violate the provisions of this policy, regardless of the success or failure of the attempt, will, in the case of staff and students, be dealt with under the terms of the relevant disciplinary procedure or policy as applicable to staff and students, and may result in disciplinary action and/or notification to the relevant law enforcement agencies.

Where a visitor or contractor violates or attempts to violate this policy, their access to the University's IT systems, network, WiFi, email and/or internet facilities shall be withdrawn and the University will, where appropriate, notify relevant law enforcement agencies. In the case of contractors, the University will seek to have the individual removed from services provided to the University, on a permanent basis.

The University also reserves the right to withdraw access from all or part of its IT systems, network, WiFi, email and/or internet facilities where it reasonably believes that this policy is being contravened.

Related Policies

Policies which should be read in conjunction with this policy are:

- IT Acceptable Use Policy
- User Account Policy
- Internet Policy
- Email Policy