

University of Gloucestershire Library, Technology & Information Service

User Account Policy

LTIU-POL-02

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 User Account Policy is to establish the rules which govern the use of the University's User Accounts (for clarity, in this instance, a User Account comprises a username and password), 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 IT systems, network, WiFi, email and/or internet facilities 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.

This policy extends to the use of any University system (hardware or software, including software as a service SaaS) which belong to the University or are leased by the University. For clarity, administrator's accounts are dealt with in a separate policy.

Please note that this policy also applies where you access the University's IT systems, network, WiFi, email and/or internet facilities 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 User Accounts as issued from time to time
- create a complex password which has a minimum of 14 characters and contains 3 of the following: capital letter, lowercase letter, symbol, numeral
- be aware that their password will never expire
- be aware that their account will be locked for 1 hour following 5 unsuccessful login attempts
- be solely responsible for all actions taken under their account
- keep the details of their account confidential and secure at all times

All Users Will Not

- share or let others use their account, or inform others of the details of their account – unless otherwise agreed with the Director of the LTI Service
- use an account other than their own – unless otherwise agreed with the Director of the LTI Service
- interfere with, or attempt to interfere with, any University User Account
- impersonate, or attempt to impersonate, any University User Account

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
- Internet Policy
- Email Policy
- Network & Wireless Policy