

University of Gloucestershire Library, Technology & Information Service

Email Policy

LTIU-POL-04

Document Control

Issue/Amendment Record

| Issue | Date of Issue | Reason for Issue |
|-------|---------------|------------------|
| 1 | 18/04/18 | Major Revision |
| 2 | 02/01/20 | Review |

Document Ownership

| | Name and Title | Signature | Date |
|----------------------------|--|-----------|----------|
| Author | Robin Livesey Content Support & Information Manager | | 02/01/20 |
| LTI Approval | Rob Blagden Director LTI Service | | 02/01/20 |
| University Approval | David James Dean of Academic Development | | 02/01/20 |
| Release Authority | Robin Livesey Content Support & Information Manager | | 02/01/20 |

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 Email Policy is to establish the rules which govern the use of the University's email system, 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 email system, 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 email system 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 email system as issued from time to time
- be responsible for all email originating from their account
- use professional language at all times
- use the out of office facility if they are going to be away from the University
- report phishing and email scams to the LTI Service via spam@glos.ac.uk

All Users Will Not

- forge email messages
- read, delete, copy or modify email directed to other users, unless specifically authorised in writing by the Director of the LTI Service
- send harassing, obscene and/or other threatening types of email (eg images of a pornographic or sexual nature, racist remarks, threats of physical violence)
- send abusive email, or email that could constitute bullying or harassment (eg on the grounds of sexuality, race, disability or age)
- send email that could constitute defamation, for example in relation to other users within the University
- send email containing 'for-profit' messages or 'chain letters'
- send email containing 'harmful' content, such as computer viruses
- send personal data via external email
- send an excess of personal messages, social invitations, jokes, cartoons or chain letters (see paragraph on Excessive Personal Use)
- put anything in an email that might bring discredit or embarrassment to the university
- knowingly respond to a phishing or spoofing email
- send confidential information to unauthorised recipients

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
- Network & Wireless Policy