UNIVERSITY OF GLOUCESTERSHIRE

University of Gloucestershire
Library, Technology & Information Service

IT Acceptable Use Policy

LTIU-POL-01

Document Control

Issue/Amendment Record

Issue	Date of Issue	Reason for Issue
1	11/12/17	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 IT Acceptable Use Policy is to establish the rules which govern the use of the University's IT systems, network, WiFi, email and/or internet facilities, 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.

Please note that this policy also applies where you access the University's network, WiFi, email and/or internet facilities through your own device.

Rules of use

All Users Will

- make themselves aware of the University's IT policies and accept their terms and conditions as applicable to them. In particular, users must familiarise themselves with the following policies:
    - IT Acceptable Use Policy (This Policy)
    - User Account Policy
    - Internet Policy
    - Email Policy
    - Network & Wireless Policy
- 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
- have read, understood, and accepted full responsibility for adhering to this policy and the relevant policies listed above as applicable
- understand that periodically unexpected system failures can occur, therefore, it is important that data files are backed up on a regular basis by users
- understand that it is the user's, and not the University's, responsibility to backup any local files that are not held on the University's central core systems
- comply with the University's instructions in relation to the usage of the University's network, WiFi, email and/or internet facilities as issued from time to time
- be aware that LTI staff may access emails or voicemail messages in the event of staff absences
- be solely responsible for all actions taken under their User ID while it is valid
- accept that data stored on the network, WiFi, email and/or internet facilities can be moved internally by qualified staff in the LTI Service for business continuity and disaster recovery purposes
- be responsible for all email originating from their User ID
- comply with the University's User Account Policy
- undertake annual data and information training (this applies to staff only)

All Users Will Not

- let others use their User ID, their Password or their University ID Card, nor inform others of their User ID or Password – unless otherwise agreed with the Director of the LTI Service or the Content Support & Information Manager
- delete, examine, copy or modify files and/or data belonging to other users without their prior consent
- deliberately impede other users through mass consumption of system resources
- take any unauthorised or deliberate action which damages or disrupts an IT system, alters its normal performance, or causes it to malfunction, regardless of system location or time duration (eg uploading a computer virus)
- forge, or attempt to forge, email messages
- attempt to read, delete, copy or modify email directed to other users without prior consent
- send, or attempt to send, harassing, obscene and/or other threatening email to another user of any email service (eg images of a pornographic or sexual nature, racist remarks, threats of physical violence)
- send 'for-profit' messages or chain letters
- use University systems to gain unauthorised access to remote systems
- attempt to gain unauthorised access to University systems from remote systems
- attempt to decrypt system or user passwords
- copy University system files
- attempt to 'crash' University systems or programs
- attempt to secure a level or privilege on university systems higher than authorised
- load programs or computer software applications onto University systems or computer hard disks without the written authorisation of the Director of the LTI Service or unless they have been granted special permission to install additional software
- wilfully introduce computer 'viruses' or other disruptive/destructive programs into the University systems or into external networks
- attempt to transfer any information, using personal or University equipment that contains content deemed to be illegal under UK law (eg child pornography, sectarian propaganda designed to incite violent acts)
- do anything which may expose the University's systems to the risk of virus infections, hacking or other unauthorised access attempts (eg disabling anti-virus software, divulging account details to others)
- install and use unlicensed software

PREVENT

The University has a statutory duty, under the Counter Terrorism and Security Act 2015, termed **PREVENT**. **PREVENT** is designed to stop people being drawn into terrorism. Users must not create, download, store or transmit unlawful material, or material that is indecent, offensive, defamatory, threatening, discriminatory or extremist. The University reserves the right to block or monitor access to such material in accordance with this policy.

In order to comply with its duty under the Counter Terrorism and Security Act 2015, the University uses specific software to **actively monitor** any attempts by users to access certain websites (for example sites promoting extremism, radicalism, violence, incitement to commit violence, sites with instructions as to how to build weaponry) and blocks access to such websites.

The University accepts that, for legitimate teaching, learning and research purposes, there may be occasions when internet access to material likely to be classified as relating to **PREVENT**, or prohibited by University policy, is required. In such circumstances, individuals should notify the Director of LTI in advance. This notification does not replace the established process for the approval of research topics.

Recording

All usage of the University's network, WiFi, email and/or internet facilities is automatically recorded by the University's computer systems. Addresses of emails and internet sites visited are logged and the content of emails and internet pages stored on the University's servers. This is an automatic consequence of the way that the University's computer systems work. This activity takes place when you access those systems both on and off campus, and whether you are using your own device or a University device.

Some of the data collected during this process may constitute your personal data, including email logs, web traffic, IP addresses and usernames.

The University **may** use these records for a number of reasons:

- ensuring compliance with the terms of this policy
- investigating breaches and potential breaches of this and any other of the University's policies
- to provide supporting evidence to verify claims made by either individuals or the University in any investigations, claims, disputes or complaints
- ensuring compliance with regulatory practice or procedures imposed or recommended by any regulatory body relevant to the University
- to comply with any relevant UK legislation
- preventing, investigating or detecting:

    - unauthorised use of the University's IT and electronic communications systems
    - misuse of the University's IT and electronic communications systems
    - criminal activities
- maintaining the effective operation of the University's IT and electronic communications systems
- ensuring the security of university data

In particular, the University may use data collected as part of the recording activities described above to support an internal investigation. Such action will only be taken provided that permission to release such information has been given by the Director of Human Resources (or nominated deputy) or the University Secretary & Registrar (or nominated deputy) or the Director of Student Services (or nominated deputy) (as appropriate). In the event that these records are used as evidence in any disciplinary action, or any other action taken against you, you will be given the opportunity to explain or challenge them.

The Director of the LTI Service may authorise access to individual accounts in the event of an information security breach, a suspected information security breach, or in order to implement measures to avoid an information security breach, or otherwise to respond to a threat to the continued sound operation of the University's IT. Additionally, the Director of the LTI Service may inform line managers, where there has been a breach of this policy involving their staff.

The University may also provide requested data to law enforcement agencies should the University be asked to support a legal investigation into criminal activity.

Please note that any attempt to circumvent Scottish, United Kingdom, European or International law using University owned facilities may result in litigation against the offender by the appropriate authorities. If such an event should occur, the University will comply fully with any requests for information connected with the litigation process.

The University will not access and use data in any way other than as set out in this policy, and in accordance with the ACAS Code of Practice.

Using personal data in accordance with data protection laws

We will hold and process your personal data in accordance with our Data Protection Policy, which can be accessed here.

Data protection laws require that the University meets certain conditions before we are allowed to use your data in conducting monitoring activities in the manner described in this policy. We take our responsibilities under data protection laws extremely seriously, including meeting these conditions. To use your personal data, we will rely on two conditions, depending on the activities we are carrying out:

- **Performance of a contract**: Where you have a contract with the University, we may need to process your data in accordance with this policy to fulfil our obligations under that contract. This includes our contract with you as a student, member of staff, visitor, or contractor.

- **Performance of a legal obligation**: The University is subject to a number of legal obligations, including under the Counter Terrorism and Security Act 2015. We may need to process your data in accordance with this policy to comply with those obligations.

Protection of vital interests

The University may process your data in accordance with this policy to protect your vital interests, or the vital interests of another person, for example, the detection of crime.

Access to and Retention of Data

The University will retain a record of your use of the University's network, WiFi, email and/or internet facilities in accordance with our data retention guidelines. These records will be kept secure and will be accessible only by staff in accordance with the section on monitoring and/or law enforcement agencies.

Retention Period Guidelines

Data Type	Retention Period
Student Email	7 months following departure
Staff Email	13 months following departure
Firewall Logs	Maximum of 90 days
Web Access Logs	Maximum of 90 days (PREVENT)
Network Logs	Maximum of 90 days
WiFi Logs	Maximum of 90 days

Further information about records management and records retention can be accessed via the Records Management information on the public website.

You have a number of rights under data protection law in relation to the way that the University processes your personal data. These rights are set out below. You may contact the Director of the LTI Service, or the University's Data Protection Officer directly – DPO@glos.ac.uk to exercise any of these rights. They will respond to any request received from you within one month of the date of the request.

Your Rights

NUMBER	DESCRIPTION OF RIGHT
Right 1	A right to access personal data held by us about you.
Right 2	A right to require us to rectify any inaccurate personal data held by us about you.
Right 3	A right to require us to erase personal data held by us about you. This right will only apply where (for example): we no longer need to use the personal data to achieve the purpose we collected it for; or where you withdraw your consent if we are using your personal data based on your consent; or where you object to the way we process your data (in line with Right 6 below).
Right 4	A right to restrict our processing of personal data held by us about you. This right will only apply where (for example): you dispute the accuracy of the personal data held by us; or where you would have the right to require us to erase the personal data but would prefer that our processing is restricted instead; or where we no longer need to use the personal data to achieve the purpose we collected it for, but you require the data for the purposes of dealing with legal claims.
Right 5	A right to receive personal data, which you have provided to us, in a structured, commonly used and machine readable format. You also have the right to require us to transfer this personal data to another organisation, at your request.
Right 6	A right to object to our processing of personal data held by us about you (including for the purposes of sending marketing materials to you).
Right 7	A right to withdraw your consent, where we are relying on it to use your personal data.

If you have any concerns regarding our processing of your personal data, or are not satisfied with our handling of any request by you in relation to your rights, you have the right to make a complaint to the Information Commissioner's Office. Their address is:

First Contact Team
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
SK9 5AF

Excessive Personal Use

The restrictions listed below apply to staff only

The University will permit limited personal use of its IT systems, network, WiFi, email and/or internet facilities. However excessive personal use is not allowed, and may result in disciplinary action. For the purposes of this policy, excessive personal use is defined as, but is not limited to, use which:

- interferes with the main business activities of the University
- jeopardises the effective operation of the University's systems and services
- interferes with the satisfactory performance of your duties
- exposes the University to legal action or risks bringing the University into disrepute
- is disrespectful and inconsiderate

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:

- User Account Policy
- Internet Policy
- Email Policy
- Network & Wireless Policy