University of Gloucestershire
Library, Technology & Information Service

Bring Your Own Device (BYOD) Policy
LTIU-POL-20

Document Control

Issue/Amendment Record

Issue	Date of Issue	Reason for Issue
1	11/03/20	Major Revision

Document Ownership

	Name and Title	Signature	Date
Author	**Robin Livesey** Content Support & Information Manager		11/03/20
LTI Approval	**Rob Blagden** Director LTI Service		11/03/20
University Approval	**David James** Dean of Academic Development		11/03/20
Release Authority	**Robin Livesey** Content Support & Information Manager		11/03/20

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 ("**LTIS**") 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.

Type of Policy

User Policy

Purpose

The purpose of this Bring Your Own Device (BYOD) Policy is to establish the rules which govern the use of devices belonging to students, staff, agents, partners, visitors and contractors which are connecting to University systems and services via the Wireless Network.

For clarification, it is not permissible for any BYODs to be physically connected to the University Network. Anyone wishing to physically connect a BYOD to the University Network must first receive written authorisation from the Director of the LTI Service, or the Head of IT Delivery. There are no exceptions to this policy. The Director of the LTI Service and the Head of IT Delivery can both be contacted via the IT and Library Helpdesk.

Scope

Any BYOD belonging to students, staff, agents, partners, visitors and contractors. Such devices include, but are not limited to, smart phones, tablets, laptops, servers, portable hard drives, USB sticks or any other fixed or mobile computing device.

For clarification, BYODs in student halls of residence do not fall within the scope of this policy.

The University reserves the right to refuse, prevent or withdraw access to devices where it considers there to be an unacceptable security, or other risk.

Anyone using a BYOD must ensure that the operating system and security software is kept up to date at all times.

Anyone using a BYOD will need to co-operate with LTIS staff should it be necessary to access or inspect the device.

The University reserves the right to access BYODs where it is suspected that there has been a security breach or a breach of any University policy.

Anyone using a BYOD must still adhere to all the other relevant IT related University policies. These are listed below.

- IT Acceptable Use Policy
- User Account Policy
- Email Policy
- Internet Policy
- Network & Wireless Policy
- Mobile & Laptop Device Policy

Support

The University takes no responsibility for supporting, maintaining, repairing, insuring or otherwise funding BYODs. The University will not be responsible for any loss or damage resulting from any support given or advice provided.

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.