Roger Williams University

Bring Your Own Device [BYOD] Policy

Scope

This policy is intended to address users of non-university owned IT devices such as smart phones, tablets, and other devices to access and store university information. This is commonly known as 'bring your own device' and referred to in the rest of this policy as BYOD.

This BYOD policy defines the acceptable use of mobile devices, specifically the use of these devices on the RWU network and those devices connecting remotely to RWU internal and cloud-based resources. RWU reserves the right to revoke the privilege of using personally owned devices if a user does not follow this policy. The primary provisions of this policy are as follows:

- Connecting a personal device to the university's O365 applications requires installation of mobile access management application on the device.
- Employees must obtain support directly from the vendor for their personal device, if required.
- The device must be used in the manner intended by the manufacturer; it cannot have been inappropriately unlocked or hacked.
- Personal devices must be protected with a pin or password access control, and locked screen enabled when inactive.
- The employee is responsible for keeping their device up to date with vendor-approved operating systems and antivirus software.
- The employee will have their device remotely wiped of O365 data if the device is lost, stolen, transferring ownership, has an incurable virus, or has been compromised by a data breach. All employees desiring to use a personal device on the RWU network must have read the RWU Acceptable Use Policy and agree to follow all requirements of that policy when accessing university resources.

Standard Number: IT.BYOD.V1
Category: Personal Devices
Owner: Information Technology
Effective: TBD
Revision History: 8/18/2021 Security Advisory Group
Review Date: 12/19/2024