Section 17: Use of Personal Computing and Mobile Devices - Bring Your Own Device (BYOD)

Northwestern State recognized the need for faculty, staff, and students to stay connected to the university. As such, the university provides remote access to many campus services including wireless access throughout the physical campus which is readily available to employees and students. This policy outlines rules and responsibilities related to using personally owned computing and mobile devices to access university services. It is intended to protect the security and integrity of NSU's data and technology infrastructure.

Acceptable Use

- NSU defines acceptable business use as activities that directly or indirectly support the academic or administrative activities of the university.
- Employees may use their mobile device to access the following NSU owned resources: email, calendars, contacts, documents, web services, etc..

Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed.
- Tablets including iPad and Android are allowed.
- Connectivity issues are supported by IS. Basic connectivity information can be found at support.nsula.edu. Users experiencing issues may contact the helpdesk.

Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device.
- The device must lock itself with a password or PIN if it's idle for five minutes.
- Rooted (Android) or jailbroken (iOS) devices are strictly forbidden from accessing the network.
- The employee's device may be remotely wiped if 1) the device is lost, 2) the employee terminates his or her employment, 3) IS detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.

Risks/Liabilities/Disclaimers

- While IS will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- NSU reserves the right to disconnect devices or disable services without notification.
- Lost or stolen devices must be reported to NSU IS Personnel within 24 hours.
- The employee is personally liable for all costs associated with his or her device.
- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of NSU and personal data due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.
- NSU reserves the right to take appropriate disciplinary action for noncompliance with this policy.

Wireless Connectivity

Northwestern State continues to expand its campus wireless network. Currently enrolled students and faculty and staff with a valid user account may make use of the university wireless network where it is available on campus. You must have a valid NSU login account in either the faculty/staff or student domain. The password is the same whether using wireless or other means to access NSU systems. Guest access is not available at this time.

Resolution of Issues Accessing or Using NSU Resources

NSU help desk personnel will work with users to determine the cause of connectivity issues. If a problem is found with NSU systems, the problem will be resolved by the appropriate NSU staff. If the problem is isolated to a user's personal computer or mobile device, it will be their responsibility to fix the problem. NSU employees will not alter faculty, staff or student's personal devices.

Procedure for addressing student technology problems:

1. The student contacts the help desk by e-mail or phone.
2. If the student help desk worker is unable to resolve the student issue, the issue is escalated to Level 2 status and assigned to the appropriate ECE staff member.
3. If the ECE staff member is unable to resolve the problem, the problem will be escalated to Level 3 status. ECE staff will contact appropriate technical support personnel in Information Systems or Student Technology. Once the Level 3 support personnel have reviewed the problem, ECE staff will contact the student with appropriate information.