Status **Active** PolicyStat ID **12704045**

Origination	12/2018	Owner	Reta Richmond: ADMINISTRATIVE ASSISTANT
Last Approved	01/2023	Area	Student Development Committee
Last Revised	01/2023		
Next Review	01/2025		

BLESSING-RIEMAN College of Nursing & Health Sciences

Student Mobile Devices

PURPOSE

To identify the student requirements necessary to mitigate risk and to protect Blessing-Rieman College of Nursing and Health Sciences (the College) from a security breach in regard to mobile devices.

POLICY

Students may choose to have a personally owned mobile device set up to access web-facing College Information Technology (IT) services such as email, calendar, or other approved apps or services. The students are required to follow all applicable College Information Security policies and procedures. All data on the student's mobile device will be erased when the pin code or password is entered incorrectly five (5) times.

PROCEDURE

Student Security Responsibilities

Students must not store confidential data on mobile devices. Students should always be aware of the physical location of any device that has College IT services on it. They must take steps to prevent loss or theft and keep the device in a secure location.

It is strongly recommended that Apple iCloud, Google Drive, or similar technology be utilized by the student to prevent the loss of data on the device such as personal photos. Backing up and preventing the loss of data on a personally owned device is solely the responsibility of the owner. Students will be required to sign a form acknowledging this policy.

Setup and Removal of IT Services

College IT provides a guide on how to set up email on the College website under IT Help Desk.

Students' accounts will be immediately deactivated upon dismissal or withdrawal from the College. Students' accounts will be terminated 90 days after graduation from the College. This will result in not being able to access email, calendar, or other approved apps or services on their mobile devices.

Configuration of Student Mobile Devices

A security configuration that requires a locking pin code or password on the device will automatically be applied when the College email account is added to the device.

The pin code or password will be set to expire every 90 days.

The security configuration will enable the data on the device to be automatically erased in the event of the wrong pin code or password being entered on the device five (5) times in a row.

Approval Signatures

Step Description	Approver	Date
Approval by College Senate	Reta Richmond: ADMINISTRATIVE ASSISTANT	01/2023
Approval by Student Development Committee	Jessica Bliven: Assistant Professor	12/2022
Approval by Student Development Committee	Andrew Griesbaum: STUDENT/ ALUMNI SERVICE OFFICER	12/2022