Rutgers School of Nursing Bring Your Own Device (BYOD) Acceptable Use Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who are connecting a personally-owned device to Rutgers School of Nursing's organization network for educational purposes. This policy is intended to provide freedom for students to use their preferred personal devices while protecting the security and integrity of Rutgers School of Nursing's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms

This device policy applies, but is not limited to all devices and accompanying media (e.g. USB thumb and external hard drives) that fit the following classifications:

- Smartphones
- Other mobile/cellular phones
- Tablet computers
- Portable media devices
- PDAs
- Ultra-mobile PCs (UMPCs)
- Laptop/notebook computers, including home desktops
- Any personally-owned device capable of storing organizational data and connecting to a network

The policy applies to any hardware and related software that is not organizationally owned or supplied, but could be used to access organizational resources. Access to and continued use requires that each user reads, signs, respects, and follows Rutgers School of Nursing's policies concerning the use of these resources and/or services.

Expectation of Privacy

The School of Nursing IT department will respect the privacy of your personal device while protecting the integrity of the confidential data that resides within Rutgers School of Nursing's technology infrastructure. This policy intends to ensure that data is stored securely on a device or carried over a secure networks thereby preventing access by unsanctioned resources.

Security

School of Nursing students using personally-owned devices and related software for network and data access will, without exception, use secure data management procedures. This requires that all School of Nursing students keep their password confidential—which means **never** disclosing passwords to anyone. To ensure privacy and security, and prevent unauthorized access, the following is required:

- The device must be password protected.
- Strong passwords must be used consisting of at least six characters and a combination of upper- and lower-case letters, numbers, and symbols.
- Sharing of passwords, PINs, or other authentication information is prohibited.
- The device must lock itself with a password or PIN if it is idle for five minutes.

Protection

To protect your personal computer from malicious acts, all computers must have anti-virus and anti-malware software installed and kept up to date and currently enabled. If your software is not up to date or disabled it may lead to an infection.

Students are responsible for keeping their computer updated with security patches/fixes from the appropriate software update services. This includes updating applications, such as MS Office, Adobe, iTunes , or Firefox. If your computer is not up to date it may lead to virus infection.

Help and Support

The IT department will assist students with connectivity issues, and can make recommendations about hardware or software issues students may experience. If the student-owned device requires maintenance, the student is responsible for taking the device to a third party vendor.

- For hardware support issues, Rutgers University recommends the use of Kite and Key.

The School of Nursing IT department will triage support calls to determine if the issue is software or hardware related. If the issue is hardware related, the student will be forwarded to the third-party support provider for maintenance.

Risk/Liabilities/Disclaimers

While School of Nursing IT will take every precaution to prevent student's personal data from being lost, students must take additional precautions, such as backing up email contacts, documents, and other data they deem important. All students are expected to use his or her devices in an ethical manner at all times and adhere to the School of Nursing's acceptable use policy.

Students are personally liable for costs associated with his or her device. All students assumes full liability for risks including, but not limited to, the partial or complete loss of 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.

User Acknowledgment and Agreement

I acknowledge, understand and will comply with the above referenced security policy and rules of behavior, as applicable to my BYOD usage of Rutgers School of Nursing services. I consent to adhere to the rules outlined therein.

Further information in regards to Rutgers University computing policies and procedures please visit https://oit.rutgers.edu/policies

Please direct questions, comments or concerns to sntechsupport@ca.rutgers.edu