Northern Virginia Community College
Information Technology
Bring Your Own Device (BYOD) Policy

Revised: 2/2014
Contact: Director, Information Technology Services at NVCC

Purpose

The purpose of this mobile device policy is to define standards, procedures, and restrictions for end users who have legitimate requirements to access college data from a mobile device connected to an unmanaged network outside of Northern Virginia Community College's direct control.

Scope

This policy applies to all Northern Virginia Community College (NOVA) employees, including full and part-time staff, faculty, contractors, volunteers, and student hires who utilize either College-owned or personally-owned mobile devices to access, store, back up, relocate or access any VCCS, College or student-specific data.

Applicability

This mobile device policy applies to, but is not limited to, all devices and accompanying media that fit the following device classifications:

- Laptop/notebook/tablet computers
- Mobile/cellular phones
- Smartphones
- Personal Digital Assistant (PDA)
- Home or personal computers used to access institutional resources
- Any mobile device capable of storing corporate data and connecting to an unmanaged network

The policy applies to any hardware and related software that could be used to access institutional resources, even if said equipment is not college sanctioned, owned, or supplied. The overriding goal of this policy is to protect the integrity of the private and confidential institutional data that resides within NOVA's technology infrastructure. This policy intends to prevent this data from being deliberately or inadvertently stored insecurely on a mobile device or carried over an insecure network where it can potentially be accessed by unsanctioned resources. A breach of this type could result in loss of student or employee information, damage to critical applications, and damage to the College's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of NOVA's direct control to backup, store, and otherwise access VCCS/College data of any type must adhere to college-defined processes for doing so.

It addresses a range of threats to – or related to the use of – College data:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive institutional data is deliberately stolen and sold.
Copyright	Software copied onto a mobile device could violate licensing.
Malware	Viruses, Trojans, Worms, Spyware and other threats could be introduced via a mobile device.
Compliance	Loss or theft of financial and/or personal and confidential data could expose the college to the risk of non-compliance with various identity theft and privacy laws.

NOVA grants its employees the privilege of purchasing and using smartphones and tablets of their choosing at work for their convenience as well as those who are provided college owned devices based on their position requirements. The College reserves the right to revoke this privilege if users do not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of NOVA's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms.

College employees must agree to the terms and conditions set forth in this policy in order to be able to connect their devices to the company network.

Acceptable Use

All NOVA employees are required to sign the Information Technology-Employee Acceptable Use Agreement and agree to abide by all applicable state, federal, VCCS, and college policies, procedures, and standards that relate to the Virginia Department of Human Resource Management Policy 1.76—Use of Internet and Electronic Communication Systems, the VCCS Information Security Standard, and the Information Technology Acceptable Use Standard. These include, but are not limited to:

- Attempting to gain access to information owned by the College or by its authorized users without the permission of the owners of that information;
- Accessing, downloading, printing, or storing information with sexually explicit content as prohibited by law or policy;
- Downloading or transmitting fraudulent, threatening, obscene, intimidating, defamatory, harassing, discriminatory, or otherwise unlawful messages or images;
- Installing or downloading computer software, programs, or executable files contrary to policy;
- Uploading or downloading copyrighted materials or proprietary agency information contrary to policy;
- Sending e-mail using another's identity, an assumed name, or anonymously;
- Attempting to intercept or read messages not intended for them;
- Intentionally developing or experimenting with malicious programs (viruses, worms, spy-ware, keystroke loggers, phishing software, Trojan horses, etc.) on any college-owned computer;
- Knowingly propagating malicious programs;

- Changing administrator rights on any college-owned computer, or the equivalent on non-Microsoft Windows based systems;

- Using college computing resources to support any commercial venture or for personal financial gain.

- The College does not permit the use of cell phones while driving a College vehicle that is in motion. It is also illegal to text and drive in the State of Virginia.

Devices and Support

- Smartphones including iPhone, Android, Blackberry and Windows phones are allowed. (* there may be some access limitations regarding Blackberry devices)

- Laptops and Tablets including Apple, Android and Windows are allowed.

- Connectivity issues are supported by IT for all College owned devices only. Personal devices are the responsibility of the owner with limited support provided at Campus computer labs or Campus IT staff.

Reimbursement

- The College does provide Cell Phone Stipends or Cell Phones on a limited basis based on specific criteria. All information regarding College cell phones and stipends can be found by reading the NOVA Cell Phone Plan Information Document .

Security

- In order to prevent unauthorized access, devices must be password protected using the features of the device. All College staff and faculty are required to maintain a strong password to access the College network.

- A strong password is defined as one that's difficult to detect by humans and computers, is at least 8 characters, preferably more, and uses a combination of upper and lower case letters, numbers and symbols. Some additional suggestions are as follows:

- Don't use any words from the dictionary. Also avoid proper nouns or foreign words.
- Don't use anything remotely related to your name, nickname, family members or pets.
- Don't use any numbers someone could guess by looking at your mail like phone numbers and street numbers.
- Choose a phrase that means something to you, take the first letters of each word and convert some into characters.

- 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.

- College employee access to College data is based on the principle of least privilege.

- Personal Identifiable Information (PII) or sensitive data should never be stored on any portable devices. This applies to College devices as well as personally owned ones.

Just as with College laptops, steps should be taken to secure your smartphones and tablets. There are numerous application tools that you can load for things such as antivirus, malware, find lost devices, website reputation and remote wipe. Some free apps are listed below but there are many others based on your OS some that are free and others that are not but tend to be more user friendly.

- Avast! Free Antivirus – For Android/Apple – performs antivirus, malware cleanup, website reputation check.
- Find iPhone/iPad – Free – For Apple devices – helps find lost/stolen devices.
- VirusBarrier – Free – For Apple Devices – performs antivirus and malware protection.
- AVG Antivirus – Free – For Android – performs antivirus and malware protection.

Risks/Liabilities/Disclaimers

- Lost or stolen devices must be immediately reported to the Vice President of Instructional & Information Technology. Employees are responsible for notifying their mobile carrier immediately upon loss of a personal device.

- All NOVA employees are expected to use his or her devices in accordance with the Information Technology Employee Ethics Agreement at all times and adhere to the College's acceptable use policy referenced above.

- The employee is personally liable for all costs associated with his or her personal device.

- The employee assumes full liability for risks including, but not limited to, the partial or complete loss of his or her personal device and its contents 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.

- NOVA reserves the right to take appropriate disciplinary action up to and including termination for noncompliance with this policy.

- Aspects of the Freedom of Information Act (FOIA) or the Virginia Public Records Act may apply to laptops, tablets, or smart phones whether personal or college owned and used for public business. For additional information see the NOVA FOIA web page.