8 BYOD USAGE POLICY

PURPOSE

The purpose of this 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 Oklahoma College's direct control. 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
- Ultra-mobile PCs (UMPC)
- 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 Northern'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 institution's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Northern's direct control to backup, store, and otherwise access corporate data of any type must adhere to college-defined processes for doing so.

APPLICABILITY

This policy applies to all Northern Oklahoma College employees, including full and part-time staff, contractors, freelancers, and other agents who utilize either company-owned or personally-owned mobile devices to access, store, back up, relocate or access any department or student-specific data. Such access to this confidential data is a privilege, not a right, and forms the basis of the trust Northern has built with its students, employees and community. Consequently, employment at Northern does not automatically guarantee the initial and ongoing ability to use these devices to gain access to institutional networks and information.

It addresses a range of threats to – or related to the use of – institutional 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.

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed and issued at the sole discretion of the Department of Information Technology.

Affected Technology

Connectivity of all mobile devices will be centrally managed by Northern's Information Technology Department and will utilize authentication and strong encryption measures. Although Northern is not able to directly manage external and mobile devices which may require connectivity to an external network, end users are expected to adhere to the same security protocols when connected to non-institutional networks. Failure to do so will result in immediate suspension of all network access privileges so as to protect the college's infrastructure.

Policy and Appropriate Use

It is the responsibility of any employee of Northern who uses a mobile device to access institutional resources to ensure that all security protocols normally used in the management of data on conventional storage infrastructure are also applied here. It is imperative that any mobile device that is used to conduct college business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that user's account. Based on this, the following rules must be observed:

Access Control

Northern reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to institutional and institutional-connected systems. Northern will engage in such action if it feels such equipment is being used in such a way that puts the college's systems, data, employees, and students at risk.

Prior to initial use on Northern's network or related infrastructure, **all college owned mobile devices must be purchased through and registered with the Information Technology Department.**

All mobile devices attempting to connect to the corporate network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by Northern's Information Technology (IT) Department. Devices that have not been previously approved by IT, are not in compliance with IT's security policies, or represent any threat to the college network or data will not be allowed to connect. Laptop computers or personal computers may only access the college network and data using a Secure Socket Layer (SSL) Virtual Private Network (VPN) connection. The SSL VPN portal Web address will be provided to users as required. Smart mobile devices such as smartphones, PDAs, and UMPCs will access the corporate network and data using Mobile VPN software installed on the device by IT.

SECURITY

Employees using mobile devices and related software for network and data access **will**, without exception, **use secure data management procedures.** All mobile devices must be protected by a **strong password (See Section 3 of IT Policy)**. **Employees agree to never disclose their passwords to anyone**, particularly to family members if institutional work is conducted from home.

All users of mobile devices must employ reasonable physical security measures. End users are expected to secure all such devices used for this activity whether or not they are actually in use and/or being carried. This includes, but is not limited to, passwords, encryption, and physical control of such devices whenever they contain college data. Any non-college computers used to synchronize with these devices will have installed up to date anti-virus and anti-malware software deemed necessary by Northern's IT Department. Any mobile device that is being used to store Northern Oklahoma College data must adhere to the authentication requirements of Northern's IT Department.

IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with Northern's Information Technology policy.

Employees, contractors, and temporary staff must erase all college related data permanently from **personally owned devices** once their use is no longer required. Divisions and departments must notify the IT Department when a **college owned device** needs a transfer in users, be replaced or is no longer needed.

In the event of a lost or stolen mobile college device it is incumbent on the employee to report this to IT immediately. IT will attempt to remotely wipe all data and lock the device to prevent access by anyone other than IT. If the device is recovered, it can be submitted to IT for re-provisioning.

Usage of location-based services and mobile check-in services, which leverage device GPS capabilities to share real-time user location with external parties, is prohibited within the workplace. This applies to corporate-owned mobile devices being used within the college premises.

HELP & SUPPORT

Northern's IT Department will support its sanctioned hardware and software, but is not accountable and will support such devices on a very limited basis and at the discretion of the Director of Information Technology for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the IT Department.

Employees, contractors, and temporary staff will make no modifications of any kind to company-owned and installed hardware or software without the express approval of Northern's IT Department. This includes, but is not limited to, any reconfiguration of the mobile device.

IT reserves the right, through policy enforcement and any other means it deems necessary, to limit the ability of end users to transfer data to and from specific resources on the enterprise network.

ORGANIZATIONAL PROTOCOL

IT can and will establish audit trails and these will be accessed, published and used without notice. Such trails will be able to track the attachment of an external device to a device, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user accepts that his or her access and/or connection to Northern's networks may be monitored to record dates, times, duration of access, etc., in order to identify unusual usage patterns or other suspicious activity. This is done in order to identify accounts/devices that may have been compromised by external parties. In all cases, data protection remains Northern's highest priority.

Northern employees must **immediately report** to his/her manager and Northern's IT Department **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

Northern Oklahoma College will not reimburse employees if they choose to purchase their own mobile devices. Employees will not be allowed to expense mobile network usage costs.