Mobile Device Acceptable Use Policy

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate business requirements to use a private or WCCCD provided mobile device that can access the college's electronic resources. 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 such as iPads
- Mobile/cellular phones
- Smartphones
- PDAs
- Any mobile device capable of storing District data and connecting to an unmanaged network.

The goal of this policy is to protect the integrity and confidential data that resides within WCCCD'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 compromised. A breach of this type could result in loss of information, damage to critical applications, financial loss, and damage to the District's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of WCCCD's direct control to backup, store, and otherwise access District data of any type must adhere to WCCCD-defined processes for doing so.

Applicability

This policy applies to all WCCCD employees, including full and part-time staff, contractors, faculty and other agents who utilize either WCCCD-owned or personally-owned mobile device to access, store, back up, relocate or access any District resources / info. Such access to the district resources / info is a privilege, not a right. Consequently, employment at WCCCD does not automatically guarantee the initial and ongoing ability to use these devices to gain access to District networks and information.

The policy addresses a range of threats:

Threat	Description
Loss	Devices used to transfer or transport work files could be lost or stolen.
Theft	Sensitive District data is deliberately stolen and sold by an employee.

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 information / 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 at the sole discretion of IT. Unauthorized use of mobile devices to back up, store, and otherwise access any college related information / data is strictly forbidden.

This policy is complementary to any previously implemented policies dealing specifically with data access, data storage, data movement, and connectivity of mobile devices to any element of the WCCCD network.

Policy and Appropriate Use

It is the responsibility of any employee of WCCCD who uses a mobile device to access District 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 WCCCD 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

1. IT reserves the right to refuse, by physical and non-physical means, the ability to connect mobile devices to District and District-connected infrastructure. IT will engage in such action if it feels such equipment is being used in such a way that puts the District's systems, data, student, staff and faculty at risk.

2. Prior to initial use on the District network or related infrastructure, **all mobile devices must be registered with IT.** WCCCD District IT will maintain a list of approved mobile devices and related software applications and utilities as needed. Devices that are not on this list may not be connected to District infrastructure. Although IT currently allows only listed devices to be connected to District infrastructure, it reserves the right to update this list in the future.

3. **End users** who wish to connect such devices to non-college network infrastructure to gain access to college data **must employ**, for their devices and related infrastructure, security measures deemed necessary by the IT department such as updated software, anti-virus software, and personal firewall. District data is not to be accessed on any hardware that fails to meet WCCCD's established IT security standards.

All mobile devices attempting to connect to the District network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by WCCCD's 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 District network or data will not be allowed to connect. Laptop computers or personal PCs may only access the District network using a Virtual Private Network (VPN) connection.

Security

4. **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 the WCCCD's password policy for additional details. **Employees agree to never disclose their passwords to anyone.**

5. 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 WCCCD data. Any non-District computers used to synchronize with these devices will have installed anti-virus and anti-malware software deemed necessary by WCCCD's IT department. Anti-virus signature files on any additional client machines – such as a home PC – on which this media will be accessed, must be up to date.

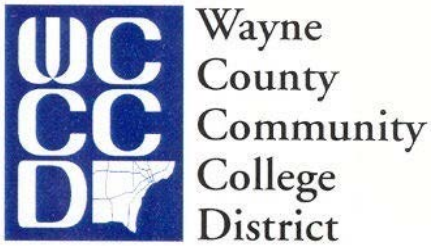
6. IT will manage security policies, network, application, and data access centrally using whatever technology solutions it deems suitable. Any attempt to contravene or bypass said security implementation will be deemed an intrusion attempt and will be dealt with in accordance with WCCCD's overarching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

7. Employees, contractors, Full time faculty, part time faculty and temporary staff will **follow all WCCCD-sanctioned data removal procedures to permanently erase WCCCD-specific data from such devices once their use is no longer required.**

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

9. Employees, contractors, Full time faculty, part time faculty and temporary staff will make no modifications of any kind to WCCCD-owned and installed hardware or software without the approval of the WCCCD Division of Information technology. This includes, but is not limited to, any reconfiguration of the mobile device.

10. Division of Information Technology 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 WCCCD network.



Organizational Protocol

11. Division of Information Technology can and will establish audit trails and these will be accessed and used without notice. Such trails will be able to track the attachment of an external device to a PC, and the resulting reports may be used for investigation of possible breaches and/or misuse. The end user agrees to and accepts that his or her access and/or connection to WCCCD'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/computers that may have been compromised by external parties. In all cases, data protection remains WCCCD's highest priority.

Policy Non-Compliance

Failure to comply with the Mobile Device Acceptable Use Policy may, at the full discretion of the College, result in the suspension of any or all technology use and connectivity privileges, disciplinary action, and possibly termination of employment.