Mobile Device Acceptable Use Policy

April 2012

Purpose

The purpose of this policy is to define standards, procedures, and restrictions for end users who have legitimate school related assignment requirements to access the internet and the Stark County District 100 network from a mobile device. 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.
- E-Book readers
- IPads and IPods
- Ultra-mobile PCs (UMPC).
- Mobile/cellular phones.
- Smartphones
- PDA's
- Home or personal computers used to access the internet and school resources.
- Any mobile device capable of storing data and connecting to an unmanaged network.

The policy applies to any hardware and related software that could be used to access the internet and school resources, even if said equipment is not District sanctioned, owned, or supplied.

The overriding goal of this policy is to protect the integrity of the private and confidential data that resides within Stark County CUSD #100'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 information, damage to critical applications, and damage to the District's public image. Therefore, all users employing a mobile device connected to an unmanaged network outside of Stark County CUSD #100's direct control to backup, store, and otherwise access data of any type must adhere to district-defined processes for doing so.

Applicability

This policy applies to all Stark County District students who utilize either district-owned or personally-owned mobile device to access, store, back up, relocate or access any information on the Districts network or the internet. Such access to this is a privilege, not a right, and forms the basis of the trust between the students, Faculty and the Technology Department. :

Addition of new hardware, software, and/or related components to provide additional mobile device connectivity will be managed at the sole discretion of the District. Non-sanctioned use of mobile devices to back up, store, and otherwise access any school -related 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 Stark County District network.

Responsibilities

The Technology Department has the authority to manage and maintain security on any mobile devices that are brought into the district for educational or non-educational purposes.

It will be the responsibility of the Faculty and Administrators to notify the Technology Department when a mobile device needs to access the internet or the Stark County District Network.

Connectivity of all mobile devices will be centrally managed by Stark County District Technology Department and will utilize authentication and strong security measures. Although students will be allowed to bring in mobile devices, failure to notify the faculty so the mobile device may connect to the school districts network will result in immediate suspension of all internet and network access privileges on the mobile device and that mobile device will not be allowed back into the Stark County District until a parent conference is completed.

The mobile devices when connected to the Stark County District's network will be filtered in accordance with the Children's Internet Protection Act. If devices are connected to the internet through a non-District internet provider there is no content filtering and the District cannot be held responsible for the content on that is accessed or downloaded on the device. Therefore the District will maintain that all mobile devices will need to be connected to the Stark County District Network through the Technology Department or those devices will not allowed in the District.

Policy and Appropriate Use

It is the responsibility of any student of Stark County District 100 who uses a mobile device to access the school network 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 school business be utilized appropriately, responsibly, and ethically. Failure to do so will result in immediate suspension of that student's privileges. Based on this, the following rules must be observed:

Security

Prior to initial use on the Stark County District's network infrastructure, **all mobile devices must be registered with** the Technology Department through the Faculty member that will be utilizing the mobile devices in their classrooms. The Technology Department will maintain a list of approved mobile devices and related software applications and utilities. Devices that are not on this list may not be connected to the Districts infrastructure.

All mobile devices attempting to connect to the District's network through an unmanaged network (i.e. the Internet) will be inspected using technology centrally managed by the Stark County Technology Department and the Districts' filtering company. Devices that have not been previously approved by the faculty are not in compliance with Technology security policies, or represent any threat to the schools network or data will not be allowed to connect. Permission will be granted on a case by case basis.

The Technology Department will manage security policies, network, application, and data access centrally using whatever reasonable and legal 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 Stark County District's Acceptable Use Policy.

In the event of a lost or stolen mobile device it is incumbent on the user to report this to the school office immediately. The school office personnel will then contact the Technology Department and access for that mobile device will be stopped. The Stark County District is not responsible for any lost or stolen mobile devices that students bring into the district.

Help & Support

Stark County District's Technology Department will support its sanctioned hardware and software, but is not accountable for conflicts or problems caused by the use of unsanctioned media, hardware, or software. This applies even to devices already known to the technology department.

Organizational Protocol

The Technology Department 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 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 Stark County District 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 and students safety are the District's highest priority.

The **end user agrees to immediately report** to his/her teacher or staff member **any incident or suspected incidents of unauthorized data access**, data loss, and/or disclosure of company resources, databases, networks, etc.

Every mobile device user will be entitled to an opportunity, but not a guarantee, to connect his/her mobile device to the Stark County District Network. While a mobile device user will not be granted access to the schools network using a mobile device without accepting the terms and conditions of this policy, students are entitled to decline signing this policy if they do not understand the policy or are uncomfortable with its contents.

Any questions relating to this policy should be directed to the Technology Coordinator or building Principals.

Policy Non-Compliance

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

Declaration

I, _____, have read and understand the above Mobile Device Acceptable Use

Policy, and consent to adhere to the rules outlined therein.

_____ _____

Student Signature Date

_____ _____

Parent Signature Date

_____ _____

Teacher Signature Date

_____ _____

Principal Signature Date