POLICY	9570 **Adopted:** March 4, 2014 **Revised:** August 6, 2015 **Personnel & Negotiations**

SUBJECT: MOBILE DEVICE MANAGEMENT POLICY

Purpose

The BOCES Board is committed to and encourages an open and collaborative environment. To this end, the BOCES provides some employees with mobile devices to enhance the services they provide to school districts. While these devices can make employees more effective, there are inherent risks in the use of mobile devices, including the ease by which these items or personally sensitive data can become lost or stolen.

The purpose of this policy is to clearly state the position of BOCES concerning mobile devices and to define user requirements necessary to mitigate these risks.

Definitions

Mobile Device: Any handheld or portable computing device including, but not limited to, a smartphone, PDA or tablet. This includes, but is not limited to the following: laptops, netbooks, iPods, iPads, Kindles, Nooks, or smartphones.

Examples of unacceptable electronic devices include, **but are not limited to**, the following: gaming devices [i.e., Nintendo 3DS, Handheld PlayStation (PSP), etc.], recording devices, radios, pagers, devices that only support WEP encryption, 802.11b only devices, and any other similar devices.

Sensitive Information: Any information that, if released to the public, could be used to cause harm or damage to either an individual or the district. Such information could include social security numbers, driver's license information, or individual financial information (such as credit card numbers, bank account numbers, or financial statements). Sensitive Information is used in this document to include high-risk, restricted and confidential information.

PIN: Personal Identification Number: This can be any combination of numbers (usually a minimum of four) that is used to unlock a device.

Remote Wipe: The ability to erase all data on a device when the user and the device are physically separated. This is most often done through a service that the manufacturer provides via a website.

Virus: A computer program that is usually hidden within another seemingly innocuous program that has the function of stealing or destroying data or causing any number of unwanted system behaviors.

Malicious Software: Often called malware, this is software designed to disrupt computer operation, gather Sensitive Information, or gain unauthorized access to computer systems.

Anti-virus Software: Software designed to detect and/or remove Malicious Software and Viruses from a computer system.

Security Patch: A fix to a program or application that eliminates a vulnerability exploited by malicious hackers. Most Mobile Devices will notify the user of updates to their installed applications that include the latest vulnerability fixes.

Policy

It is the responsibility of anyone who utilizes the GST BOCES internal network for the purpose of accessing or processing Sensitive Information using a Mobile Device to take appropriate measures at all times to safeguard that information. An individual who uses the GST BOCES network and configures a personal mobile device to access district data is responsible for securing or removing the data on the device if the device were to be compromised, lost, or if the individual has its relationship with BOCES terminated. All such individuals ("Users") will ensure they are taking every reasonable precaution against accidental or intentional data compromise by implementing the standards below. Users must also implement the standards below.

Standards

- All use of Mobile Devices, which utilize GST BOCES network resources, will be subject to the Acceptable Use Policy for Computing and Network Resources.
- If possible, all devices will be updated to the latest device operating system with the latest Security Patches.
- In addition to the above security settings, all Users are expected to use their device in an ethical manner. Using a device in ways not designed or intended by the manufacturer is not allowed. This includes, but is not limited to, "jail-breaking" or "rooting" the device. Devices that are "jail-broken," "rooted," or hacked will not be permitted on the network.

- All applications (apps) will be updated with the latest Security Patches.
- All devices will be configured with a PIN or password-enabled lock screen configured to activate at no more than 10 minutes of inactivity.
- All devices will have Remote Wipe enabled either through ActiveSync, a third party app or MDM solution, or the manufacturer's website.
    - A remote wipe may be used in the event of involuntary or voluntary termination of employment. During the exit interview process, ActiveSync data and all other Sensitive Information must be removed from all personal mobile devices and validated by the appropriately appointed GST BOCES personnel.
- Users will immediately notify the GST BOCES Helpdesk or IT support team should they believe that their device has been lost, stolen, or otherwise compromised so that appropriate actions to safeguard data and the GST BOCES Network can be enacted.
    - If the BOCES suspects a security breach related to a Personal Device, it may take any and all actions deemed appropriate to secure data, and the GST BOCES Network, including, but not limited to, disconnecting the device from the network and remote wiping the device.
    - A remote wipe may also be used in the event that the mobile device is lost or stolen.
- All devices that have been used to store, access and/or process Sensitive Information will be wiped to remove such data before they are transferred to someone else through sale or gifting.

Guidelines

- Users should make sure they know the location of their Mobile Devices at all times. Mobile Devices should not be left unattended.
- Users should not allow someone who is not authorized access to the GST BOCES network to use their devices if they are used to process Sensitive Information.
- Users should install and regularly update Anti-virus Software.
- Users should learn how their Mobile Devices function. Not all users are aware that when they open an attachment from email most devices will store a copy of this attachment somewhere on the device. Users should consult the device user manual and other sources to learn how the device handles data.

- It is good practice to use a Mobile Device only for transitory storage of Sensitive Information. Users should delete any Sensitive Information stored on their devices immediately after the work with it is completed.

The BOCES assumes no responsibility for the loss of, theft of, or damage to any personal mobile device.