Appendix B – Best Practices When Using Smart Phones and Other Mobile Devices

- Be certain to password protect all mobile devices. Many give you the option to use simple, 4-digit passwords or strong passwords. Turn on strong passwords if available.

- Keep your device current with operating system and app updates.

- Turn on or set up the feature to remotely wipe/erase your device if available. As an example, Apple iOS devices like the iPhone and iPad have a free service called "Find Your iPhone or iPad." This service gives the user the ability to erase the device, should it be lost or stolen, thus keeping potentially important data out of strangers hands.

  http://www.apple.com/mobileme/features/find-my-iphone.html

- Do not root your Droid or jailbreak your iOS device. This will void your warranty.

- When installing an app, pay attention to what it needs access to. While there have not been widespread reports of virus activity and/or Trojan apps, those behaviors are possible. Do not give the app access to data on your device it does not need. Some apps may need to access your GPS location, contacts, or email in order to operate successfully, but often they do not.

- University owned devices still require you to have a personal account tied to that device for downloading apps. Note that when the device is returned to the University, you will lose all the apps and data on that device, even if paid for by your own funds.