Guidelines for Smartphones & Mobility

Mobile computing devices and smartphones (Android, iPhone, iPad, etc.) provide the ability to access information remotely and to communicate using various methods. Designed primarily for convenience, many of these communication methods, as well as the devices themselves, can also be very insecure. The following guidelines are applicable to any mobile device that is capable of communicating using wireless technology, including Bluetooth, 802.11/'WiFi' and cellular data networks.

Support Limitations

Colby Information and Technology Services (ITS) currently supports the Android and Apple iOS (iPhone/iPad/iPod) mobile platforms and employ management capabilities that owners of college-issued phones should be aware of. If you use a college-issued iPhone/iPad or Android device, do not hesitate to contact the support center with any questions about these guidelines. Colby ITS does not officially support other mobile platforms and cannot always offer technical assistance on employing some of these guidelines on unsupported devices.

General Security

- **Never use a mobile device to store sensitive data and/or documents.** In addition to being far more insecure than standard computers, mobile devices can be easily lost, misplaced or stolen. If sensitive data must be accessed on a mobile device, it should be done so remotely (remote file access or secure web browser).
- **Activate screen locking and/or pass code protection.** This does not protect your device and data in the event of theft, but it will prevent someone from picking up your device and immediately having access to it. For convenience, some devices allow for a timer before the password lock is engaged—this timer should not exceed 15 minutes.

- **In the event of loss, theft or misplacement, wipe out the phone remotely.** If you have a college-issued device, ITS can perform this service for you. Even if you believe you've just misplaced the phone—it is better to be safe than sorry. Your data will be intact should the phone be recovered. If you have a non-supported mobile device, there are features and commercial products (not supported by ITS) that can also perform this service.

Communications Security

- **Avoid using Bluetooth, and never in public places.** Bluetooth is an extremely insecure protocol, and even with its limited range can present significant vulnerabilities to your conversations and personal data. Tether or sync devices to your computer using a USB cable instead of Bluetooth. Don't use Bluetooth headsets as they can be easily eavesdropped—use a wire instead.
- **Secure 802.11 'WiFi' connections as you would your computer's connection.** The same technology begets the same security guidelines:
    - **Disable the wireless connection when not in use.** This conserves battery life and prevents the device from using open and insecure wireless networks.
    - **Use wireless encryption.** Use WPA or WPA2 encrypted networks, such as the 'Colby Access' network, instead of open and insecure networks.
        - If you have a choice between your cellular provider's data network and a public WiFi network, consider using the provider's network—even if slower, it is more secure.
        - If you must use an unencrypted network, be aware that your communications may be eavesdropped—when performing online tasks, assume your activities are open to nearby users.

Software and Application Security

- **Use secure protocols and connections wherever possible, especially e-mail.** Configure communication programs, such as e-mail and calendar sync, to use encryption whenever possible—this will ensure that your

personal communications are encrypted even when using open, public networks.

- **Do not store e-mail on the device.** It is recommended that you employ IMAP mail so that electronic mail is not stored on the phone beyond a certain range of dates. E-mail containing sensitive information and/or attachments should be deleted as soon as possible so as not to remain resident on the mobile device.
- **Exercise caution when installing third-party software.** The ease at which new applications can be installed on mobile platforms also makes it easy to install unwanted or vulnerable software. Make sure you trust the publisher of any software that you install on your device.
- **Avoid ‘parking’ your device on a sync connection with a host computer.** When your device synchronizes, it forms an insecure partnership with your computer and potentially opens additional pathways to your desktop or laptop. Once the device is synced with the host computer, terminate the connection until another sync is needed.