

MOBILE DEVICE POLICY

Applicability: This policy applies to all Oak Hill employees who are required to hold Oak Hill issued cell phones, as well as all Oak Hill employees with email accounts who use their personal “mobile devices” (full-feature mobile phones with mini keyboards and PC-like capability that support e-mail, texting, calendaring, and/or Internet functionality), iPads®, tablets or other mobile devices for Oak Hill purposes.

A. Overview.

Oak Hill recognizes that many employees who are required to hold Oak Hill cell phones have opted to use their personal “mobile devices” instead. Oak Hill further understands that mobile phone technology is convenient and a feasible alternative for conducting Oak Hill business. This policy addresses Oak Hill’s expectations for employees with respect to securing any Oak Hill data that may reside on an employee’s mobile device. Oak Hill will not reimburse employees for the costs of using their personal mobile devices for company business.

B. Policy.

1. Restrictions to Email Server.

Employees with Oak Hill email accounts may not synchronize their personal mobile devices to Oak Hill’s email server without the approval of their department head. In exchange for such permission, such employees shall comply with the security guidelines set forth below and complete the attached authorization form to be maintained in the IT department. Additionally, such employees shall authorize Oak Hill to install software that will enable Oak Hill to locate and disable the mobile device in the event that it is lost or stolen. Oak Hill expressly disclaims any obligation to either replace or repair the device or the data contained on it should the disabling software be used.

2. No Right of Privacy in Business Use.

Employees who use mobile devices for business purposes and who are witnesses in any arbitration, litigation or regulatory investigation may be subject to any lawfully issued subpoena for Oak Hill data (e.g., voicemail messages, text messages, emails, internet access) stored on the device.

3. Security.

Oak Hill employees who use any mobile devices to access Oak Hill information over a cellular or internet connection are responsible for securing their devices to prevent sensitive data from being lost or compromised, viruses being spread, and other forms of abuse of Oak Hill’s technology infrastructure. The loss or theft of a personal mobile

device that contains program participant information covered under the HIPAA laws may result breach notification requirements pursuant to Oak Hill's HIPAA policies. Therefore, if any mobile device is lost, stolen, or believed to be compromised, the incident must be reported to the General Counsel/Privacy Officer and IT immediately.

The following guidelines ensure that Oak Hill employees have a clear understanding of proper procedures and usage of mobile device access to Oak Hill's servers and systems. Oak Hill reserves the right to modify this guideline to address any concerns that can potentially cause a disruption of services to Oak Hill's server.

A. Protect Your Mobile Device. To ensure that data accessed through your mobile device is secure, especially in the event that it is misplaced, stolen or believed to be compromised, all Oak Hill employees who access Oak Hill's email server must comply with the following:

- Use a "PIN" consisting of at least six (6) characters. It is recommended that the PIN be a combination of letters, numbers, and special characters.
- Set the timeout for the PIN to a maximum of 30 minutes. Some devices allow this setting to be adjusted to be more or less than 30 minutes.
- Limit the number of attempts to enter the PIN correctly five (5). If the PIN is entered incorrectly five (5) times, the device will have to be reset to "factory settings" to be unlocked.
- Password should be changed periodically; recommended time is every 6 months.

B. Install Antivirus Software. Although rare, mobile devices are just as susceptible to viruses as desktop or laptop computers. Not all mobile devices have anti-virus software, but a number of vendors do offer antivirus and anti-spam solutions for some devices. Oak Hill encourages employees to install such anti-virus and anti-spam software on mobile devices.

C. Use Encryption. Account and password information passed over any wireless network should always be encrypted. If your device supports encryption, enable it and make sure that your sensitive documents are encrypted. Some devices will automatically encrypt these documents and others will present you with the option.

D. Disable Unused Options and Applications. Reduce security risks by limiting the use of your device to only necessary applications and services. In addition, other benefits are extended battery life, increased memory storage, increased application performance, efficient synchronization time and reduced management of security updates for applications. Bluetooth and Infrared (IR) are services that should be configured properly or turned off because they can potentially pose a risk to your device and data.

E. Perform Regular Data Backups. Back up your data on a regular basis in case your mobile device is lost, damaged or loses battery life. Make sure Oak Hill data is backed-up on Oak Hill's server and not your personal computer.

F. Dispose of Your Device Safely. When you are ready to dispose of your device or return it to the vendor, be sure to remove all sensitive information first. The device should be restored to "factory defaults" which can be accomplished by a "hard reset."

G. Charge Your Mobile Device. When not in use, always charge your mobile device. The loss of power can potentially cause all stored information to be erased.

Cross-reference: Telephone, Facsimile and Cell Phone Use

This policy was approved on March 30, 2011

This policy is effective on April 15, 2011

**EMPLOYEE AUTHORIZATION TO ALLOW
OAK HILL TO REMOTELY WIPE PERSONAL CELL PHONE
AND RELEASE**

Employee Name: _____
Department/ Cost Center _____

Cellular telephone number: _____

Cellular telephone service provider: _____

Brand/model of mobile device (e.g., Droid, iPhone, Blackberry)

Contract termination date: _____

I, _____, hereby agree to promptly notify IT in the event that my mobile device is lost or stolen. In such case, I hereby authorize Oak Hill, its employees and agents, to remotely wipe clean my mobile device. I acknowledge and agree that Oak Hill is not responsible for the cost of repairing or replacing my phone in the event that it is rendered unusable as a result of its efforts to remove Oak Hill data.

Employee Name (printed)

Employee Signature

Date: _____