ALGONQUIN COLLEGE | Information Technology Services

# MOBILE PHONE SECURITY SAFEGUARDS

Employees that receive mobile phones provided by the College must ensure that the phone and data stored within, such as email, email attachments, and files, are protected by appropriate security safeguards at all times. This is to prevent security incidents that can result in costly student and employee personal data breaches, unwanted negative media attention and corporate brand damage, among other risks.

Algonquin College only uses Apple mobile phones because of the enhanced security safeguards that they provide over Android mobile phones. Apple devices are encrypted by default; operate on closed, protected ecosystems; the Apple Store apps are inspected before publication; and the devices are more frequently updated with operating system and security patches.

## Implementing Initial Security Safeguards:

The following safeguards must be implemented *before* the mobile phone is removed from purchasing.

- ☐ **Create an Apple ID and strong password** using your Algonquin College email address and office telephone number. You may not use a personal email address. This allows the mobile phone to be securely wiped and reused when it is returned.
  - **To configure during setup, follow these steps:** Swipe or Press home to open → Select Your Country or Region → Enable or Disable Location services → Create a Passcode → Set Up as New iPhone → Enter your Apple ID and Password.
  - **To configure in iOS Settings:** Settings → Sign in to your iPhone at Top → Enter your Apple ID and Password
  - **If you don't have an Apple ID configured, select:** Don't have an Apple ID? → Create Apple ID
- ☐ **Create a 6-digit passcode:** Settings → Touch ID and Passcode → Turn Passcode On.
- ☐ **Disable applications that can be accessed from the lock screen (e.g. Wallet)**: Settings → Touch ID & Passcode → (Disable applications)
- ☐ **Enable the "Erase Data" setting** to configure the device to automatically erase its content and settings after more than 10 failed passcode attempts: Settings → Touch ID & Passcode → Erase Data at Bottom

## Additional Safeguards

- ☐ Only download applications that you trust. Review the privacy statement before doing so. Periodically remove apps that you do not use.
- ☐ Download the AC Mobile Safety App. Refer to: http://apparmor.com/clients/algonquincollege.com/
- ☐ Install the College's recovery software application: http://www.frontdoorsoftware.com/algonquin/
- ☐ Set up Find my iPhone to help recover your phone if it is lost: Settings → (Your Name at Top) → iCloud → Find My iPhone → Enable
- ☐ Ensure your device is up to date – Settings → General → Software Update
- ☐ Ensure your important information is backed up – Settings → Account → iCloud → iCloud Backup
- ☐ While a personal choice, the use of a fingerprint for authentication is not recommended, due to risks associated with digitized biometrics becoming stolen.

For information regarding Algonquin College's information security policy (IT05), please refer to: http://www.algonquincollege.com/policies/policy/college-information-security/.

For additional assistance, please contact the Cyber Security Unit (CSU), Information Technology Services (ITS).

*Information Security is everybody's business*