Guidelines 4

Mobile Device Encryption - iOS

Approved by ISWG 12 June 2017

Introduction

Most recent Apple devices already encrypt their contents by default, having different levels of protection. Encrypting your Apple device with a passcode, fingerprint or pattern to access your phone is advised to help protect the data on your device such as your email, photos and any files or documents. In the unfortunate event of losing your Apple device it is very important that no one can access your personal or LSHTM data. If you lose an LSHTM purchased device, or lose any device which contains LSHTM data, the loss should be reported immediately to csirt@lshtm.ac.uk. To help you comply with the policy please read these guidelines in conjunction with the LSHTM Policy on Mobile and Remote working http://www.lshtm.ac.uk/its/informationsecurity/policy/lshtm_mobile_and_remote_working_policy.pdf. This requires any mobile devices that have personal data (any data that can identify a living individual) be encrypted.

iOS versions

To check what version of iOS you are currently running go to **Settings > General > About**. You can then see it under the iOS version. Apple automatically sends a notification on devices when it is time to update your iOS version. Should you wish to update this in your own time please go to **Settings > General > Software Update**, click on **Download > Install**.

Please note: The iOS version update will not be successful if the battery is less than 50% charged therefore please have your device fully charged and that the update is done via a secure Wi-Fi connection. Please go to the link for further information on updating your iOS version https://support.apple.com/en-gb/HT204204

iOS version	Initial release date
iOS 10	September 13th, 2016
iOS 9	September 16th, 2015
iOS 4	June 2010

How to set up encryption on device

Apple uses powerful device encryption from iOS 8 version (2014). It is recommended that you update your device from iOS 4 version. Once your Apple device is encrypted, all data stored on the device is locked behind the passcode or fingerprint. This is known only to its owner therefore it is important that you do not forget this. Please follow the steps below to encrypt your phone:

- Go to Settings.
- Touch ID & Passcode (On devices without Touch ID, go to Settings > Passcode).
- Tap turn passcode on.

- You have the option to enter a 6-digit passcode or you can tap Passcode Options to use the 4-digit numeric code, a custom numeric code, or a custom alphanumeric code.
- You will need to enter your passcode to confirm and activate this.

After the passcode is set you need to scroll down to the bottom of the screen and verify that "that protection is enabled" is visible.

To enable screen lock

- Go to Settings.
- Display & Brightness.
- Scroll to and tap auto lock.
- Select the time out option of your choice (2 min, 5 min..)
- Tap General to then set the lock screen timeout.

How to check your Apple device has been encrypted successfully

Now to confirm if encryption is enabled or not:

- Go to Settings.
- Touch ID & Passcode.
- Scroll to the bottom of the screen.
- Here you should see "Data protection is enabled".

Your Apple device should now be fully encrypted.

Find my iPhone/iPad

In the event of losing your Apple device there is a way of locating the device and remotely wiping the contents of the device if required. For this to work the lost Apple device needs to be enabled. The device will also need to be switched in and connected to the internet for you to be able to remotely wipe this.

- Start at your Home screen.
- Tap Settings > iCloud.
- Scroll to the bottom and tap Find My iPhone.
- Slide to turn on Find My iPhone and Send Last Location.

Locate device

- Sign into iCloud - https://www.icloud.com/.
- Open Find My iPhone, and select a device to view its location on a map.
- Locate your device and switch on Lost Mode.
- From here you can track, lock and wipe your device contents.
- Further information can be found on https://support.apple.com/kb/PH2700?locale=en_US.