

Mobile Device Encryption – Android

Approved by ISWG 12 June 2017

Introduction

Encryption protects your information stored on your phone such as your email, photos and any files or documents. In the unfortunate event of losing your device it is very important that no one can access your personal or LSHTM data. Encrypting your phone with a passcode, password, fingerprint or pattern to access your phone is advised to help protect the data on your device. 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.

Android versions

The OS version for smartphones is currently Nougat which was made available August 2016. Please find below the older versions of android OS and their release dates:

Code Name	Version number	Release date
Nougat	7.0 - 7.1.1	August, 2016
Marshmallow	6.0 -6.0.1	October, 2015
Lollipop	5.0 – 5.1.1	November, 2014
Kitkat	4.4 – 4.4.4	October, 2013

It is recommended that the OS version is checked on your device to ensure that it is up to date with the latest software, and that this is compatible with your android device. To check or update your android system please follow the steps below:

Go to Settings > About phone > System updates

If you have an older device the android version might not be able to update and you may need to get a newer device as a replacement.

How to set up encryption on device

You need to ensure that your device is connected to a secure Wifi and has been charged.

Important: Once an Android device is encrypted, all data stored on the device is locked behind the PIN code, fingerprint, pattern, or password known only to its owner therefore it is important that you do not forget this.

Passcode to enable

Enabling a passcode ensures that, in case of the loss of the device, nobody else can then use your device or access the data on the device. You should use a strong password. We strongly recommend using a password as the type of screen lock and the password should:

- Be at least 6 characters long and not be a dictionary word (in any language)
- Utilise mixed case, numeric and/or special characters

Screen lock to enable

- Go to settings.
- Tap on Security.
- Tap on Screen Lock.
- Choose the type of screen lock you would like (Pattern, Pin, Password, fingerprint recognition) and enter the passcode twice to enable it.

Auto-Lock to enable

If your device is left unattended for a certain amount of time then auto lock can be setup to ensure that your device cannot be accessed by anyone but yourself. Please also ensure that the auto lock time is set to less than 10 mins. To set this up:

- Go to settings.
- Tap on Display.
- Tap on Sleep.
- Select time limit.

Remote Tracking/Location to enable

If your device is lost there is a function to remotely track where it is and also to remotely wipe this (erase all data). Please note that for this to work, the device needs to have the remote tracking to be set up beforehand, it has to be switched on and also have internet working via mobile data or Wi-Fi. To set this up:

- Go to Settings > Google > Security.
- Turn **ON** "Remotely Locate this Device and "Allow Remote lock and erase".
- Turn **ON** "Location History" to timeline the places that you have been.
- Settings > Google > Location > Google Location History > turn ON.

Track

- Go to <https://www.google.co.uk/android/devicemanager>.
- Sign in with your Google account.
- This will auto track your device.
- View your location history by going to <https://www.google.co.uk/android/devicemanager>.

How to check the device has been encrypted successfully

You can check the encryption status of a device by opening the Settings app and select Security from the options. There should be a section titled Encryption that will contain the encryption status of

your device. If it's encrypted, it will read as such. If not, it should read similar to "encrypt device."
Tap on the option if you want to encrypt your device. Please note that encrypting your device can take up to an hour.