Newcastle University
How to secure an Android v4 mobile device

Introduction

This guide shows you how to secure a laptop, tablet or smartphone running Android v4.0. These changes need to be made if your device is used to:

- Collect, store or process confidential or sensitive data
- Access your University email

The settings detailed in this guide may differ between Android devices. If this is the case then you need to check your instruction manual.

This guide shows you how to:

- Backup your Android device
- Password protect your device
- Configure the screen lock
- Display a message on the lock screen
- Encrypt your device
- Encrypt your SD card
- Protect your device from malicious software

You should read this document in its entirety before making any of these changes.

By following the guidance in this document you are helping to improve compliance with the University’s Information Security and Data Protection Policies.

You should also read the information security guidance on the ISS web site at:
http://www.ncl.ac.uk/itservice/security
1. Backup your device

Before you make any changes to your device you need to backup your important work. To do this:

- Connect your Android device to your PC

- Click on the “Windows Start” button and open “Computer” or double click on the “Computer” icon on your “Windows Desktop” (Fig 1)

- You should see your device listed under “Portable Devices” (Fig 2). Right click on your device and select “Open in new window”. This should open another window that shows your device as a drive (Fig 3).

- Copy your important work to your H: drive or other appropriate backup location. We recommend that you back up your important work on a regular basis.
2. Setup a password

A password needs to be setup if your device is used to collect, store or process confidential or sensitive data or used to access University email. You can do this by making the following changes:

In “Settings” (Fig 4), “Security”, “Screen security”:

- Open “Screen Lock” (Fig 5) and Select “Password” (Fig 6)

**IMPORTANT NOTE**

Be very careful when entering your password. You might accidentally lock yourself out of your device if you make a mistake.

Enter a password that is at least eight characters long, contains a mix of upper-case and lower-case characters, and contains at least one number and one special character (e.g. !, *, $, &, etc...). An example of such a password is Ncl*2013
3. Protect your password

Your password is the only thing that stops someone from accessing the contents of your device if it’s lost or stolen:

- Avoid writing your password down. If you do down write down your password, never store your password with your device.

- Do not forget your password. We are unable to recover data from a password protected device.

- Criminals might be able to guess your password from the fingerprints left on the screen. After using your device, wipe the fingerprints off your screen with a dry cloth that doesn’t scratch.

4. Configure the screen lock

Configure your device to automatically lock after two minutes of inactivity and when the power key is pressed.

In “Settings”, “Security, “Screen security”:

- Make sure that “Lock instantly with power key” is ticked (Fig 7)

- Open “Lock automatically” and select “2 minutes” (Fig 8)
Fig 7, configuring your Android device to lock instantly when the power key is pressed.

Fig 8, configuring your Android device to lock after two minutes of inactivity.
5. Display a message on your lock screen

Configure your device to display a message on the lock screen

In “Settings”, “Security”, “Screen security”:

- Open “Owner information” (Fig 9) and enter a message to be displayed on your lock screen (Fig 10). Make sure that your message includes your name and a contact telephone number or email address.

- Make sure that “Show owner info on lock screen” is ticked.

![Fig 9, the “Owner information” option](image)

![Fig 10, entering a message to be displayed on your lock screen](image)
6. Encrypt your device

Encryption needs to be setup if your device is used to collect, store or process confidential or sensitive data or used to access University email. You can setup encryption by making the following changes:

In “Settings”, “Security”, “Screen security”:

- Open “Encrypt device” (Fig 11) and then press the “Encrypt device” button (Fig 12). You will be asked to confirm your password
• You will now be asked to confirm the encryption of your device. Make sure that “Fast encryption” is not ticked and then press the “Encrypt device” button. Your device will restart and display an encryption progress bar.

![Fig 13, confirming the encryption of your Android device](image)

7. Encrypt your SD card

Encryption of SD cards needs to be set up if your device is used to collect, store or process confidential or sensitive data or used to access University email. You can setup encryption by making the following changes:

In “Settings”, “Security”, “Screen security”:

- Open “Encrypt SD card” [Fig 14] and make sure that “Encrypt SD card” and “Full encryption” are ticked [Fig 15]. Also make sure that “Exclude multimedia files” is not ticked.

- Select continue and enter your password

- On the “Enable SD card encryption” screen and click “Apply” [Fig 16]
How to secure an Android v4 mobile device

Fig 14, the “Encrypt SD card” option

Fig 15, configuring SD card encryption
8. Protect your device from malicious software

You are strongly advised not to install apps from outside “Google Play” (previously called the “Android Market”). Doing so may leave your device vulnerable to attack from malicious software. Malicious software may lead to a breach of your own privacy or may result in the theft of your confidential and sensitive data.

If your device is used to collect, store or process confidential or sensitive data or used to access University email, then you need to install and run antivirus software that is in receipt of the latest antivirus updates.

9. Storing data in the cloud

Many Android devices provide software for storing data in the cloud. It is important to know that cloud-based storage can carry information security risks. Before storing any data in the cloud, you should read the ISS information security web page on cloud computing:

http://www.ncl.ac.uk/itservice/security/emailinternet
10. The dangers of allowing other people to use your device

You are strongly advised not to let anybody else use your device. Doing so could place your confidential and sensitive data and University email at risk of unauthorised access and disclosure.

11. Information security incidents

If your device is lost or stolen, and that device contains confidential or sensitive data, then you must notify the ISS Information Security Team through the ISS Service Desk by email (it.servicedesk@ncl.ac.uk) or by telephone (0191 222 5999). It may be possible for us to remotely erase the contents of your device if it is used to access University email.

12. Security checklist

<table>
<thead>
<tr>
<th>Ref</th>
<th>Requirement</th>
<th>✔</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Have you backed up your device?</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Have you setup a password?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Do you know how to protect your password?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Have you configured your lock screen?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Have you displayed a message on your lock screen?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Have you encrypted your device?</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Have you encrypted your SD card?</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Do you know how to protect your device from malicious software?</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Do you know why you need to be careful when storing data in the cloud?</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Do you know why you should not let anybody else use your device?</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Do you know how to report a lost or stolen device?</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Have you read the University’s Information Security and Data Protection Policies?</td>
<td></td>
</tr>
</tbody>
</table>