Introduction

This guide shows you how to secure an Apple device running iOS6 such as an iPad, iPhone or iPod. 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 Apple devices. If this is the case then you need to check your instruction manual.

This guide shows you how to:

- Backup your device
- Setup iCloud
- Remotely locate, lock and erase your device
- Stop the export of sensitive and confidential data to iCloud
- Passcode protect your device
- Encrypt your device
- Turn off Picture Frame
- Restore your device if anything goes wrong
- Keep your system software and “Apps” up to date

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. Back-up your device

Before you make any changes you need to backup the contents of your device so that you don’t lose any data or “Apps” if anything goes wrong. You can do this by synchronising everything on your device with iTunes (Fig 1).

Fig 1, synchronising your device with iTunes
2. Setup iCloud and turn on find my iPad, iPhone or iPod

By turning on “Find my iPad, iPhone or iPod” you can locate your device on a map and remotely lock or erase it if it gets lost or stolen. You can do this by making the following changes to your device “Settings” (Fig 2):

- In "Settings > Privacy" (Fig 3)
  - Turn “Location Services” “ON”

- In "Settings > iCloud" (Fig 4)
  - Enter your Apple ID logon details or “Get a Free Apple ID” if you don’t already have one
  - After you have entered your Apple ID logon details, select “OK” when asked to “Allow iCloud to Use the Location of Your iPad, iPhone or iPod”
  - Turn “Find my iPad, iPhone or iPod” “ON”
3. How to locate, lock or erase your device if it’s lost or stolen

If you have lost a device that’s setup to use iCloud, then you can use the iCloud web site to locate, remotely lock and erase that device:

Open Internet Explorer (if you are using a Windows PC) or Safari (if you are using an Apple Macintosh) and go to:

- **www.icloud.com** and login using your Apple ID (Fig 5)

![Fig 5, the iCloud web site](image)

- **Click “Find My iPhone”** (Fig 6)

![Fig 6, the iCloud web site showing the “Find My iPhone” icon](image)
• Click “Devices” (Fig 7)

![Fig 7, the “Find My iPhone” map showing the “Devices” button](image)

• Click on your iPad, iPhone or iPod in the “Devices” drop down menu (Fig 8)

![Fig 8, your device shown in the “Devices” drop down menu](image)
If your device is connected to a WiFi or mobile network, it should be shown as a green target (Fig 9). If your device is nearby, but you are having problems finding it, then you can make your device:

- Play a sound by clicking “Play Sound”

If your device is not connected to a WiFi or mobile network, then you will see a grey target showing the last known location of your device.

If you still can’t find your device then you can:

- Lock the device and have it display a message by clicking “Lost Mode”
- Or you can wipe all data from the device by clicking “Erase iPad, iPhone or iPod”

Your device will be placed in “Lost Mode” or will be erased the next time it connects to a WiFi or mobile network.

Fig 9, the location of your device with options to “Play Sound”, place into “Lost Mode” or “Erase” the device
4. Stop the export of confidential and sensitive data to iCloud

Certain types of data cannot be exported to the cloud (e.g. you may have signed a non-disclosure agreement or sharing of the data may be controlled by research council regulations).

To prevent confidential and sensitive data from being exported to the cloud:

In "Settings > iCloud > Photo Stream" (Fig 10)

- Turn “My Photo Stream” “OFF”
- Turn “Shared Photo Streams” “OFF”

In "Settings > iCloud > Documents & Data" (Fig 11)

- Turn “Documents & Data” “OFF”

In "Settings > iCloud > Storage and Backup" (Fig 12)

- Turn ”iCloud Backup” ”OFF”

Fig 10, Turning off “Photo Stream”
Fig 11, Turning off “Documents & Data”

Fig 12, Turning off “iCloud Backup”

For more information on securely using the cloud, please refer to the ISS Information Security web page on cloud computing: http://www.ncl.ac.uk/itservice/security/emailinternet
5. Passcode protect your device

A passcode 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 a passcode by making the following changes:

In "Settings > General" Select “Passcode Lock” (Fig 15):

- Turn “Simple Passcode” “OFF”
- Select “Turn Passcode On” and type in a new passcode
- Enter a passcode 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 passcode is Ncl*2013
- Change "Require Passcode" to "Immediately"

Fig 15, setting up a passcode

6. Protect your passcode

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

- Avoid writing down your passcode. If you do down write down your passcode, never store your passcode with your device.
- Do not forget your passcode. We are unable to recover data from a passcode protected device.
- People might be able to guess your passcode 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.
7. Encrypt your device

Encryption 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 > General > Passcode Lock" [Fig 16]:

- Turn "Erase Data" "ON"
- Underneath the "Erase Data" option the following system messages need to be displayed:

  "Erase all data on this device after 10 failed passcode attempts"
  "Data protection is enabled"

Data protection is a layer of encryption that cannot be broken by “jail breaking” your device and will protect everything stored on your device.

Fig 16, enabling “data protection” encryption by turning on “Erase Data”
8. Turn off picture frame

The Picture Frame needs to be turned off to stop your device from showing pictures on the lock screen. This is important because some pictures might contain confidential or sensitive data. The following steps will allow you to turn the Picture Frame off:

- In "Settings > General > Passcode Lock" (Fig 17):
- Turn "Picture Frame" "OFF"

Fig 17, turning off the "Picture Frame"
9. Keeping your software up to date

By keeping your iOS system software up to date, you are ensuring that your device is in receipt of the latest security updates. You can update your iOS system software by completing the following steps:

In "Settings > General" (Fig 18)

- Open “Software Update”

Your device will let you know if it’s running the latest version of iOS, or if a later version is available to download and install.

You should also check that all your Apps are kept up to date by opening the “App Store” and checking if any updates are available to download and install.
10. **Backing up your data**

Make sure you keep a copy of all your important work on the ISS Filestore. This will ensure your work can be recovered if your device is lost, damaged or stolen.

11. **Restoring your device if anything goes wrong**

If you have previously backed up your device, then you can use that backup to restore your device if anything goes wrong.

To restore your device from a backup:

- Connect your device to your computer
- Open iTunes
- Open your device’s “Summary” and click “Restore Backup” (Fig 19)

![Fig 19, the restore from backup option](image)

12. **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.

13. **The dangers of “jail breaking” your device**

You are strongly advised not to “jail break” your device. Doing so would invalidate your device warranty and 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.

14. **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.
15. 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 turned on find my device?</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Have you familiarised yourself with the iCloud web site?</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Have you stopped the export of confidential and sensitive data to iCloud?</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Have you set up a passcode?</td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Do you know how to protect your passcode?</td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Have you encrypted your device?</td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Have you turned off Picture Frame?</td>
<td></td>
</tr>
<tr>
<td>9</td>
<td>Do you know how to keep your device up to date?</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>Have you backed up all of your important work to the ISS Filestore?</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Do you know how to restore your device if anything goes wrong?</td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Do you know why you should not let anybody else use your device?</td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Do you know why “jail breaking” your device is dangerous?</td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Do you know how to report a lost or stolen device?</td>
<td></td>
</tr>
<tr>
<td>15</td>
<td>Have you read the University’s <a href="#">Information Security</a> and <a href="#">Data Protection</a> Policies?</td>
<td></td>
</tr>
</tbody>
</table>