Quick Reference Sheet
Secure and encrypt an Android 4 mobile device

**Introduction**
This guide shows you how to secure and encrypt an Android 4 mobile device if it is used to collect, store or process confidential or sensitive data or is used to access University email.

If you have problems securing your device then please download our more detailed guidance document. Relevant sections are referenced by page number.

By securely configuring your device you are helping to improve compliance with the University’s Information Security and Data Protection Policies.

**Cloud Storage**
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). Care should be taken to stop protected data from being uploaded to the cloud.

For more information on securely using the cloud, please refer to the ISS Information Security web page on cloud computing.

**Security Incidents**
If your device is lost or stolen and contains confidential or sensitive University work, then you must immediately notify the ISS Service Desk by telephone (0191 222 5999) or email (it.servicedesk@ncl.ac.uk).

It may be possible for us to remotely erase the contents of your device if it is used to access University email.

- **Backup your device**
  (Page 2)
- **Mount your device as a drive and copy your important work to your H: drive or other appropriate storage location**

**Set up a password**
(Page 3)
- In “Settings > Security” Open “Screen Lock” and select “Password”

**Configure the lock screen**
(Page 4)
- In “Settings > Security” Tick “Lock instantly with power key”

**Display a message on your lock screen**
(Page 6)
- In “Settings > Security” Select “Owner information”

**Encrypt your device**
(Page 7)
- In “Settings > Security” Select “Encrypt Device”

**Encrypt your SD card**
(Page 8)
- In “Settings > Security” Select “Encrypt SD card”

**Note:**
Always keep a master copy of your important work on the ISS Filestore or other appropriate storage location. This will allow you to recover your important work should anything go wrong.

**Note:**
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. An example of such a password is Ncl*2013

**Note:**
Enter a message that contains your contact telephone number or email address

**Note:**
Your multimedia files may contain sensitive or confidential information that needs to be encrypted.