Quick Reference Sheet
Secure and encrypt an Apple Macintosh running OS X 10.8

Introduction
This guide shows you how to secure and encrypt an Apple Macintosh running OS X 10.8 if it is used to collect, store or process confidential or sensitive data or is used to access University email.

By securely configuring your computer 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 your iCloud or other cloud service.

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 important work
Copy your important work to your H: drive or other appropriate storage location

Set up a password if you don’t already have one
Click “Security & Privacy”, then click “General”
Click “Change Password” and then tick “Disable automatic login”

Configure your lock screen
In “System Preferences”
Click “Security & Privacy”, then click “General”
Tick “Require password” and change the text to “immediately”

Encrypt your computer
In “System Preferences”
Click “Security & Privacy”, then click “FileVault”
Click “Turn On FileVault”

Turn on your firewall
In “System Preferences”
Click “Security & Privacy”, then click “Firewall”
Click “Turn On Firewall”

Install Apple security updates
Open the “Apple” menu and select “Software Update”

Install anti-malware software
Install anti-malware software from a trusted and recognised company and keep it up to date

Write down your recovery key
Your recovery key can be used to access your data if you are accidentally locked out of your computer

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

Tick “Show a message when the screen is locked” and enter a message that contains your contact information

Tick “Require password” and change the text to “immediately”

Click “Firewall Options” and tick “Block all incoming connections”

Click “Firewall”
Click “Turn On Firewall”

Install anti-malware software from a trusted and recognised company and keep it up to date

Note:
ISS and your local computing support can advise on appropriate anti-malware software

Note:
Keep your recovery key safe and secure by keeping it in a locked filing cabinet. Never store your recovery key with your computer