Supporting Apple Tech

Best Practices for Security and Mobility at Faculty of Education
The University of Auckland
William McGrath
Mac Usage: Students

- **OS X**: 77%
- **Windows**: 23%

$n = 39000$ in March 2012 accessing FoEd Moodle
Mobile Usage: Students

$n = 1400$ in March 2012 accessing FoEd Moodle
Mac Usage: Staff

49% iMac
51% DELL

n = 759
Mac Usage: Staff

n = 750
Mobile Usage: Staff

$n = 126$
Mobile Usage: Staff

- iPhone: 89%
- Other Smartphone: 6%
- BlackBerry: 6%

$n = 105$
Policy, policy, policy

shall be secured in a manner that is considered reasonable and appropriate to the level of sensitivity, value and criticality that the Institutional Data has to the University.

c. Individuals who are authorized to access Institutional Data shall adhere to the appropriate related guidelines.
   - laptop set-up
   - data replacement

REVIEW AND REVIEW AND REVIEW

Finally, there are the risks (reputation, commercial, privacy and others) associated with the exposure or loss of sensitive, unique or personal information contained. The loss this represents, although difficult to assess, has the potential to:
   - student or staff personal details
   - any information that the user would wish to remain private

Objectives:
   - To ensure:
     - informed
     - medic information
     - sensitive information

To counter these risks, laptop security must be addressed in five ways:
   - user responsibility; through increased user awareness of the risks and application of a laptop security interim standard (this document)
   - physical security; both at the user's "base" and when travelling
   - access control/authentication;
   - data protection; using software and hardware based solutions
   - tracking/recovery; particularly for devices at high risk or containing very sensitive data
Access Control

FOED
Apple Citizenship in a Microsoft world
Strategy

MDM
It all starts here...

- `foed_bind_ad.sh`
- `foed_bin`
- `enable_filevault.sh`
- Profile installation
Example: Mac Lab

- Needs to be shutdown every night at 8pm
- Needs to be on at 7am
- Prevent access to system preferences
- A session “skeleton”
- Software Update settings
Example: Staff notebook

- Software Update settings
- Password enforcement
- Screensaver enforcement
- Other key settings (wifi)
Example: Lecture Theatre

- Software Update settings
- “Kiosk mode” Finder (User can logoff/reboot, not shutdown)
- System Prefs etc
Settings Management
Secure Wipe/Lock
Web Clips
All this means nothing...
Scenario

- MacBook left in general common area - stolen
- No screensaver password
- No firmware password
- User has local administrator rights
- iPad left in office under paperwork - user “misadventure”
Backups
Full disk encryption

FileVault 2
The Padlock
Screen Savers

- A login password has been set for this user
- Require password immediately after sleep or screen saver begins
- Show a message when the screen is locked
- Disable automatic login

Allow applications downloaded from:
- Mac App Store
- Mac App Store and identified developers
- Anywhere

Click the lock to make changes.
Local Admin Policy

uid=500(derpina) gid=20(staff), 80(admin)
Bonus for champs!
What next?

- Munki for software management
- out of box deployment
- moving away from SOEs
- moving towards "thin imaging"

File Storage - what next?
More Info

• William McGrath
  w.mcgrath@auckland.ac.nz

• @talesonrails

• http://about.me/wmcgrath