SECURITY WITH PLYMOUTH UNIVERSITY

Technology & Information Services

SEC-GDL-006-Mobile Computing Guidelines

Author: Paul Ferrier

Date: 12/02/2015

Document Security Level: **PUBLIC**
Document Version: 0.90
Document Ref: SEC-GDL-006
Document Link:
Review Date:

SEC-GDL-006-Mobile Computing Guidelines

Introduction

Mobile devices are increasingly used for University activities and the security of such equipment must be maintained in order to manage and prevent unacceptable risks arising to the University and other information assets through the use of unapproved or unsafe working facilities.

The physical protection and software safeguards that are available within the University environment are not automatically available when working outside of that environment. There is an increased risk of information being subject to loss or unauthorised access. Mobile computing users must take special measures to protect sensitive information in these circumstances.

These guidelines have been developed to promote good information security practices outside the boundaries of the University's premises, including working at home and in public areas.

1. Definitions

Mobile devices	are any portable electronic device (including but not limited to laptops, tablets, smart phones etc.) that is capable of storing, processing or transmitting information.

2. Remote connection to the University network

2.1 Guidelines for both Windows and Mac users are provided for secure connection to the University, through the Computing Policies[1] on the intranet.

These guidelines should be followed if you are attempting to access data classified as Standard (for use both staff and/or students, that should not be publically available) or Restricted (only available to named users).

3. Information security risks

3.1 Standard or Restricted data on mobile devices should be kept to a minimum to reduce the risk and impact should a breach of security occur. Data should be transferred to the University network as soon as practical and not held on the mobile devices storage medium.

3.2 Mobile devices are vulnerable to theft, loss or unauthorised access, particularly when taken outside of the University's physical environment. They should be provided with appropriate forms of protection to prevent unauthorised access to their contents, such as:

- 3.2.1 Password protection (or other safeguard) should be in place to ensure that access is restricted to the authorised user of the device
- 3.2.2 Screen saver or standby protection (for example, screen saver or hibernation requiring password on wake) should be applied
- 3.2.3 When standard information is required to be held for an extended period of time, or restricted information is held on mobile devices, data encryption must be used to protect either the information itself, or preferably the entire device
- 3.2.4 Full disk encryption offers the maximum protection for sensitive information on laptops and other devices and should be used where the sensitivity of data requires it. Alternatively and where appropriate, data can be encrypted at the partition level or virtual partition (a file encrypted to behave like a disk partition) level. In most cases, encrypted virtual partitions or disks can be copied to USB pens, CDs and DVDs for safe transportation.
  Note that data is only protected by encryption when the laptop is powered off and not in

[1] Computing Policies (requires a University account to access)

normal use.

3.3 Personally owned mobile devices should not be used for business activities without appropriate security measures, including up to date security "patches" and antimalware (anti-virus and malware) protection.

3.4 USB memory sticks are prone to loss or theft. Add-on encryption to these devices can be left turned off. The product recommended by the University is Ironkey. This has inbuilt encryption which cannot be turned off, is resistant to physical disassembly and destroys the data after 10 failed attempts to access.

3.5 Public Cloud Storage such as (but not limited to) DropBox, iCloud, Google, OneDrive and Box should only be used with caution, due to the differing native levels of security that they provide. It is advised that if you have a business need to store information in a cloud environment that you read the Data Classification Policy[2] (EIM-POL-001), as this will assist in the decision making process.

3.6 Loss of any University issued mobile device must be reported immediately to your Line Manager.

3.6.1 If the device contained standard or restricted information, this should also be reported immediately to Technology and Information Services and the Data Protection Officer at the University.

3.7 When undertaking mobile computing the following guidelines must be followed:

3.7.1 When travelling, equipment (and media) must not be left unattended in public places. Mobile device should be carried as hand luggage when travelling.

3.7.2 When using a laptop, avoid processing personal, sensitive or restricted data in public places or exercise additional caution when doing so, for example, on public transport.

3.7.3 Passwords or other details for access to the University's systems should never be stored on mobile devices where they may be stolen or permit unauthorised access to information assets.

3.7.4 Security risks (for example, of damage or theft) may vary considerably between locations and this should be taken into account during use.

3.8 When a University issued device is no longer required, it must be returned to the organisation in a working state with no user allocated passwords still in place that prevent access to support staff for cleansing.

Document Control							
Version	**Author**	**Position**	**Details**	**Date/Time**	**Approved by**	**Position**	**Date/Time**
0.9	Paul Ferrier	Enterprise Security Architect	Created the document	12/02/2015			

[2] Data & information standards & policy