UNIVERSITY OF EXETER

Draft Policy for
Information on laptops and portable media

Document Control

File Name	info security policy portable2 v002.doc
Original Author(s)	Paul Sandy
Current Revision Author(s)	Paul Sandy

Version	Date	Author(s)	Notes on Revisions
0.02	Jan 2012	Paul Sandy	Minor updates.
0.01	Oct 2011	Paul Sandy	New shortened document with separate laptop / portable media and data access / transfer policies. Incorporating comments from Gary Stringer. Encryption no longer an opt-in for laptops. Added information on timescales for implementation.

1 INTRODUCTION

Overall, the University's Information Security Policy is intended to provide a pragmatic, workable policy that provides an optimum level of security while remaining compatible with the day-to-day activities that need to be carried out to run the University. An ultra-secure but cumbersome or impractical policy will simply be ignored by users and, ultimately, any security is only as strong as the weakest link.

The security of information on laptops and portable media is rightly seen as a high risk area. This document provides Policy and guidance to cover the security of this area.

Other relevant documents are listed in Section 6.

2 DEFINITIONS

These definitions may apply to more than one area of Policy. **Portable device** means any of:

- Laptop computer, notebook computer, netbook, etc
- PDA
- Tablet
- Phone, smartphone, MP3 player or other communications / audio / video device with data storage or data access capability

For the purposes of this document, **laptop** means any of:

- Laptop computer
- Notebook computer
- Netbook computer
- ie all portable computer devices typically running one or more of Windows, MacOS, Unix / Linux. Other types of mobile device are covered by other policies (LINK).

Portable medium means any of:

- CD, DVD, floppy disk, tape, zip disk, etc
- external hard disk
- USB memory stick
- Solid-state or other storage card (eg CompactFlash, SD, other new digital storage, etc)

As new devices and media emerge, the distinctions between these categories may become less clear.

Personal information (based on the definition used for Data Protection legislation purposes) is defined as any information relating to a living individual who can be identified either from the data, or from that information used in conjunction with other information that may be available.

Confidential information is privileged or proprietary information that could cause harm (including reputational damage) to the University or individual(s) if compromised through alteration, corruption, loss, misuse, or unauthorised disclosure.

3 IMPLEMENTATION TIMESCALES

A programme has been underway since Spring 2011 to identify high priority laptops and / or high profile users with eligible devices and these machines are being encrypted. New laptops supplied by Exeter IT have encryption enabled.

This policy will become mandatory as of 31 December 2012. The use of unencrypted laptops or portable media after this date will be treated as a breach of this policy.

4 INFORMATION SECURITY POLICY

The University's Information Security Policy will eventually consist of sections covering all relevant activities. This policy document relates only to laptop computers and portable media.

4.1 Aims

This policy is intended to ensure that any information used or accessed by staff is protected against unauthorised access or modification when stored or accessed on any portable device or medium. There can be no absolute guarantees where security is concerned but on the whole the standard required is that such information must not be ‘readily accessible’ by any unauthorised person or persons.

4.2 Applicability

This policy applies to all staff working for, or on behalf of, the University and includes direct employees, employees of other organisations working for or in association with the University of Exeter, associates and contractors or other third parties with legitimate access to University data or systems.

Staff must take personal responsibility for adhering to this policy and should treat University information with (at least) the same care that they would expect to be applied to any personal or confidential information held about them. The Information Security Policy sits alongside other University policies which must also be adhered to (eg Data Protection, equipment disposal, arrangements when leaving or changing School or Service, etc).

Note that this policy is designed to provide an adequate level of confidentiality of data for most users. If ‘military grade’ security is required for specific projects or activities then those users for whom this is a requirement may need to implement additional security to the standard required by the parties with whom they are working.

4.3 Laptop Policy

This applies to laptop computer devices as defined above.

4.3.1 All University laptops and similar devices must be encrypted to at least the required University specification (LINK).

4.4 Portable Media Policy

4.4.1 No personal or confidential information shall be stored on any non-University portable medium except as explicitly provided for in contracts with third parties providing goods or services to the University.

4.4.2 No personal or confidential information shall be stored on any portable medium unless at least one of the following conditions is met:

1. The storage medium is encrypted to at least the required University specification (LINK).
2. Unencrypted portable media are used only in a single location and are kept securely locked away at all times when not in use. (Note that such activity carries some inherent risk of loss or breach of confidentiality of the data so anyone working in this way must be made aware of the dangers.)
3. An alternative stronger level of protection is in place if required by other agencies.

Note that, owing to the risk of user error, we do not recommend the use of an unencrypted storage medium where confidential or personal information is stored in encrypted folders or files.

5 REQUIRED SECURITY

The current list of security solutions is available on the web. This consists of encryption software for laptops and specific makes and models of USB device. See Reference 6.1.

6 REFERENCES

6.1 www.exeter.ac.uk/as/it/regulations/infosec/devices