LIVERPOOL
HOPE
UNIVERSITY
Est. 1844

Portable Data Device Security

Policy

Document Control

Date	Revision/Amendment Details & Reason	Author
July 2010	Initial Document approved by Council	M Beecroft
October 2014	Updated policy	M Beecroft
25th November 2014	Approved by University Council	

Background

Every staff member and student member who moves University data onto portable devices and other removable media is responsible for the data stored, processed and/or transmitted. The user is required to follow the security requirements set forth in this policy and in the Information Security Policy.

Purpose of this policy

If data held on portable devices is obtained by unauthorised entities, the University could be exposed to reputational damage and / or legal action e.g. under the Data Protection Act. This policy sets out the procedures which should be followed by staff and students to prevent such exposure.

Definitions

Portable Data Device: These are any devices which can be carried by hand and be used for mobile computing either in their own right or by being connected to and removed from other computing devices. They include but are not limited to laptop, notebook, tablet, mobile phone, digital cameras, USB Memory Sticks, external hard drives, CD Rom, DVDs and other storage devices

Sensitive Data: All data other than data not containing either personal information or information of a confidential nature.

Examples of Sensitive Data include:

- Medical records
- Student data
- Bank account numbers
- other personal financial information
- Personnel and/or payroll records

Policy

No sensitive data should be held on a portable device unless it is necessary for a University business reason.

If sensitive data is held on a portable device, it should be kept to a minimum.

If sensitive data is held on a portable device, the device should be provided by the University and be protected by suitable encryption software as approved by IT Services

Procedures

1. Users have the responsibility to protect the sensitive data from unauthorised use, disclosures, access, loss, corruption, damage or destruction and to adopt all proper and sensible precautions in their handling of such data

2. The definitive version of all work related data should be held on the University’s secure network storage. Portable devices should not be used as the sole storage location for any University data.

3. Confidential data may not be held on a portable device unless formal permission has been granted by the individual’s Rectorate member. Any data held on portable devices should be encrypted or the file should be protected by a password.

4. Only information which is required to be accessed off-site should be placed on portable devices. If a document is changed while on a portable device, it should be copied to the secure network storage at the earliest opportunity.

5. Any data held on portable devices should be stored for the minimum time possible and all reasonable precautions should be taken to prevent unauthorised disclosure or copying.

6. Sensitive data will not be processed, opened, read or loaded on public access computers

7. Sensitive data will not be transferred to, stored or processed on portable devices which can be accessed by third parties unless such parties have a business relationship with the University and appropriate contractual arrangements are in place.

8. **Prior to** use or display of Confidential Data via laptop computer or other portable data devices, the following security measures must be in place:
    - The device must authenticate the user before access to services is permitted.
    - Mobile devices must be configured to timeout after 15 minutes of inactivity and require re-authentication before access to services is permitted.
    - The authentication mechanism(s) must not be disabled.
    - The encryption option must be enabled on laptop computers that transmit or store University confidential information.
    - Laptops must be protected with antivirus software, updated each time the device is logged on

9. Accessing or storing data on portable devices which do not comply with the security measures listed above is prohibited regardless of whether the equipment is owned or managed by the University.

10. Portable devices should not be left unattended and logged in. Users should either log out or lock the machine using Ctrl/Alt/Delete followed by the “lock computer” button.

11. Users must adhere to safe computing practices when working off campus. In particular, appropriate measures need to be taken when connecting a portable device to the Internet.

12. Users must take all reasonable precautions to avoid the physical theft or loss of portable devices. These should not be left unattended in public places or left visible in a locked vehicle

13. Before disposing of a portable device, the User must ensure that all copies of data have been deleted including, where appropriate, those held on the hard drive.

14. In the event that a portable device containing confidential data is lost or stolen, the loss or theft must be reported immediately to the University Secretary’s Office

15. Any security breach of data should be reported to the University Secretary’s Office immediately

16. In reporting any incidents, the user must provide in writing:- ▯ The type of device
    - the nature and extent of the data
    - the security measures which were taken to protect the device and the data