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 |
| February 2017 | Updated policy | M Beecroft |
| May 2018 | Updated policy | M Beecroft |
| July 2018 | Updated Document approved by Council | M Beecroft |

## Background

Every staff member and student who moves University data onto portable devices and other storage 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 General Data Protection Regulation. This policy sets out the procedures that must be followed by staff and students to prevent such exposure.

A breach of this policy may result in serious action using the University's disciplinary policies, irrespective of any penalties or sanctions which may be imposed by the Information Commissioner in respect of failure to protect personal or Special Category data.

## Definitions

**Portable Device:** These are any devices that can be carried by hand and be used for mobile computing either in their own right or by being connected to / removed from other computing devices. They include, but are not limited to, laptop, notebook, tablet, mobile phone, digital cameras

**Portable Media:** Hand portable items used to store data in electronic form including USB Memory Sticks, plug in external hard drives, CD Rom, DVDs and other storage devices

**Confidential Data:** Information about or connected to the University's business which the user has an obligation to treat as confidential and protect from unauthorised use, access or release

**Personal Data:** Any information about any living, identifiable individuals

**Special Category Data:** All data containing either personal information or information of a confidential nature. Examples of Special Category Data include:

- race
- politics
- religion
- health

## Policy

Whenever possible, Confidential, Personal or Special Category Data must be held on the University's network systems, must be accessed and managed using only those systems and must not be downloaded for storage or remote manipulation on portable devices or media.

Under no circumstances should Confidential, Personal or Special Category Data be held on the hard drive ("C" Drive) of a portable device.

If it is essential to access Confidential, Personal or Special Category data on a portable device / media or where use of portable media is the only viable option for processing such data, the device / media must comply with the following:

- it must have been procured via IT Services. Under no circumstances can such data be transferred / accessed on any other device / media.
- Prior to transferring / accessing such data onto a University funded device / media, it must have been inspected by IT Services and formal approval given that the device / media includes the required level of security.

IT Services will maintain a list of all devices which have been certified to be used for tasks involving Confidential, Personal or Special Category data. This list will detail the devices which have been allocated to each individual user. Users must not allow anyone else to use the equipment allocated to them.

Devices which are not on the list must not be used for tasks involving Confidential, Personal or Special Category data.

## Procedures

1. Users have the responsibility to protect 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 must be held on the University's secure network storage. Portable devices must not be used as the sole storage location for any University data.

3. If data is downloaded onto portable devices / media, whenever possible, it should be anonymised / pseudonymised.

4. In relation to e-mail, items which include Confidential, Personal or Special Category data or have attachments with such data should be deleted at the earliest opportunity. Personal e-mail accounts should be reviewed on a continual bases to ensure that items are deleted in a timely manner

5. Confidential, Personal or Special Category data must not be held on a portable device unless formal permission has been granted by the individual's Rectorate member. Wherever possible, any data held on portable devices must be encrypted and the file must be protected by a password.

6. Only information that is required to be accessed off-site and that cannot be accessed via the University's remote logon facilities can be placed on portable devices or media. If data is changed whilst on a portable device, it must be copied to the secure network storage at the earliest opportunity and then deleted from the portable device / media immediately.

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

8. Confidential, Personal or Special Category data must not be processed, opened, read or loaded on public access computers.

9. Confidential, Personal or Special Category data must not be transferred to, stored or processed on portable devices that can be accessed by third parties unless such parties have a business relationship with the University and appropriate contractual arrangements are in place.

10. **Prior to** use or display of Confidential, Personal or Special Category Data via portable devices or media, the following security measures must be in place:

| **Device / Media Type** | **Requirement** |
|---|---|
| Laptop, Tablet, Notebook or equivalent | Device must use Whole Disk encryption |
| Mobile Phone | Power on password / pin; auto time out keyboard lock; encryption if available |

| | |
|---|---|
| USB Memory Stick | Hardware based encryption with software to setup and manage the passphrase to use media |
| CD / DVD | Must be encrypted prior to storage |
| Other devices that allow storage of files e.g. iPad, iPod, MP3 | Power on password / pin; auto time out keyboard lock; encryption if available. These devices must not be used unless they offer protected storage whilst in transit. iPods and MP3 do not offer this protection. |

In addition:

- 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.
- Laptops must be protected with antivirus software, updated each time the device is logged on
- IT Services can request for any portable device / media to be returned to the department for inspection and, where appropriate, update of the security on the item

11. 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.

12. Portable devices must not be left unattended and logged in. Users should preferably log out or, as a minimum, lock the machine using Ctrl/Alt/Delete followed by the “lock computer” button.

13. 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.

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

15. In the event that a User no longer requires the device / media allocated to them, the device / media must be returned to IT Services for review and subsequent reallocation. Under no circumstances should a user pass the device / media directly to another user and neither should a user accept a device from anyone other than IT Services.

16. When a portable device / media is to be disposed of, it must be returned to IT Services. Under no circumstances should a user dispose of the device / media themselves. IT Services will ensure that all copies of data have been deleted.

17. In the event that a portable device / media containing Confidential, Personal or Special Category data is lost or stolen, the loss or theft must be reported immediately using the GDPR Data Breach Reporting Procedures

18. Any security breach of data must be reported immediately using the GDPR Data Breach Reporting Procedures

19. 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

**Policy Review**

This policy will be reviewed on an annual basis to identify any required revisions.