Portable Devices and Removable Media Acceptable Use Policy - v1.0

Organisation	Oxford Brookes University
Title	Portable Devices and Removable Media Acceptable Use Policy
Creator	Information Security Working Group
Approvals Required	1. Information Security Working Group 2. CIO 3. Executive Board
Version	Version 1.0
Owner	Executive Board
Subject	The formal approved policy for the acceptable use of portable devices and removable media by University staff for the processing of University data
Rights	Public
Review data and responsibility	Annually by Information Security Working Group

1. Statement of Policy

Oxford Brookes University aspires to the highest standards of corporate behaviour, professional competence and best practice in its approach to computing and data security. The University has policies relating to Information Security[link] and Data Protection[link]. These policies require staff and students and all who have access to, and process, the University's data to keep information secure and to protect personal data. This policy relates specifically to the movement of University data from the University's systems to portable devices and other removable media and the processing of University data on such devices and media. The policy of the University is that information must continue to be kept secure and personal data must continue to be protected when it is transferred on to, or processed on, portable devices and other removable media and during any process of transfer to and from such devices or media.

2. Definitions

2.1 Portable devices and removable media are any devices which can easily 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 laptop and notebook computers, tablet computers, mobile phones, digital cameras, digital audio devices, portable hard drives, CDs, DVDs, SD

cards, memory “sticks” and flash drives.

2.2 For the purpose of this policy data can be divided into two categories:
- non-sensitive data, which is data not containing either personal information or information of a confidential nature, and;
- sensitive data, the default category, which comprises all other data, the loss of which would, or would be likely to, cause damage or distress to the University or to individuals.

Data is assumed to be sensitive unless proven otherwise. This policy relates to sensitive data.

3. Policy Principles

3.1 The dominant principle governing the use of portable devices and removable media is:

- Do not transfer the University’s sensitive data on to or store such sensitive data on portable devices or removable media unless it is **necessary** for a University business purpose and you have the explicit authority of your Head of Department.
- If it is necessary for sensitive data to be transferred on to or for such data to be stored on portable devices or removable media then the data should be minimised as much as possible, **and**
- The portable device or removable media containing the sensitive data should be an Oxford Brookes device and be protected by encryption software in line with the advice and the assistance of the University’s IT department (Oxford Brookes Information Solutions - OBIS) to the appropriate current standard.

Data minimisation means minimising the quantity and breadth of data and, where possible, anonymising personal data.

3.2 All portable devices and removable media provided by the University to its staff shall be protected by encryption software.

3.3 Staff will ensure that all such devices are protected by a secure password and that the password-protected auto-locking feature (where present) is enabled. Advice on secure passwords can be obtained from the University’s IT department OBIS.

3.4 The University will abide by legislation and regulations relating to obtaining, using, storing, protecting and disclosing data required in the pursuance of University business.

3.5 The University will provide appropriate organisational and technical measures to help keep data secure and to prevent loss, damage and destruction, assisting staff to implement such measures by producing relevant guidance.

3.6 Individuals processing University data have a responsibility to protect the data from

unauthorised use, disclosure, access, loss, corruption, damage or destruction and to adopt all proper and sensible precautions in their handling of sensitive and personal data.

3.7 Any individual using portable devices and removable media must ensure that sensitive or personal data are not compromised by inappropriate use of insecure facilities and storage.

3.8 Individuals transferring data on to or storing such data on portable or removable devices shall ensure they have the appropriate authority and approval to do so.

3.9 Sensitive data shall not be processed, opened, read or loaded on public access computers.

3.10 The University's sensitive data will not be transferred to, stored or processed on portable devices or removable media where those data are to be used or accessed by third parties unless such parties have a business relationship with the University and appropriate contractual arrangements are in place.

3.11 Anti-virus precautions should be maintained in all use of removable media devices.

4. Authorisation Process

4.1 For sensitive University data to be transferred on to or stored on a portable device or removable media for use by a member of staff appropriate authorisation shall be obtained from that member of staff's Head of Department.

4.2 The risks associated with transferring data onto a portable device or storing data on it must be assessed and controls to mitigate the risks must be identified and implemented where appropriate.

4.3 The member of staff will complete the appropriate authorisation request and secure the necessary authorisation prior to the data being placed on the portable device or removable media.

4.4 The appropriate authorisation form can be accessed here[link].

5. Guidelines

5.1 Make sure that you understand what your responsibilities are by consulting the University's Information Security and Data Protection policies. If you need further training on data protection matters, get in touch with the University's Information Compliance Officer to arrange a session.

5.2 Before using mobile computing devices to process University data, consider whether such processing is necessary. Can it be done without using a mobile device? If it can and the mobile

processing is not necessary, then adopt a more appropriate and secure alternative.

5.3 If processing data on a mobile device is necessary, consider whether the data can be minimised, or personal data anonymised, in any way.

5.4 Avoid using removable media devices for permanent or indefinite storage. Make sure data are transferred as soon as possible to a secure, permanent data store and securely removed from all intermediate media. Do not put yourself in a position where sensitive data may be lost irretrievably without a backed-up copy held in a secure University data store.

5.5 Consult your manager to ensure that you have appropriate approval to transfer data on to or to store such data on a mobile device. In order to authorise the transfer of sensitive data on to a mobile device, the Head of Department will need to know that it is necessary and that OBIS guidance has been followed on the appropriate technical measures to keep the data secure.

5.6 If you are a manager, make sure you are aware of any mobile processing carried out by your staff and that the policy is being applied. If you identify that the policy is not being applied despite appropriate briefing and training, then you will need to escalate the matter through your own senior manager, involving HR if necessary.

5.7 Consult the University's IT department OBIS (email: obis-security@brookes.ac.uk; tel. ext. 3311) for advice on defensive computing and managing any risks. OBIS will help to identify and implement any appropriate technical measures, including encryption, to ensure the security of the data and/or the device. Specific measures will depend upon the nature of the device.

5.8 Take appropriate physical precautions against the theft or loss of portable devices and removable media. If it is necessary to travel by car with such devices, as well as making sure technical measures such as encryption have been applied, make sure the devices are locked out of sight in the boot of the vehicle. If kept at home, devices still need to be kept secure to protect from opportunistic theft or access.

5.9 If a mobile computing device is disposed of, make sure that the data are properly purged and destroyed. Seek advice from the University's IT department OBIS to ensure that the data are destroyed. Guidance is available in the university's Policy on Secure Disposal of IT Equipment and Information.

5.10 Software on portable devices and removable media are subject to the same audit procedures as other computer systems. Make sure you have appropriate authority and licence for use.

6. Reporting Data Security Breaches and Lost or Stolen Portable Devices or Removable Media

6.1 All staff should report lost or stolen devices immediately to their line manager and to the University's Information Compliance Officer. This will enable an assessment to be made of any loss of data held on the device.

6.2 Any security breach of data (or suspected breaches), including those involving portable devices or removable media, should be reported immediately by email to obis-security@brookes.ac.uk or to the OBIS Service Desk at service.brookes.ac.uk or by telephone on ext. 3311.

6.3 A data security breach occurs when there is unauthorised or unlawful processing of sensitive data, including personal data, or there is accidental loss, or destruction of, or damage to such data.

6.4 In reporting the loss or theft of a device and data you are required to identify in writing
- the type of device
- the nature and extent of the data, and
- the security measures which were taken to protect the device and the data

Authorisation form for the transfer of data to a portable device or to removable media

This is a request to transfer University sensitive data to and to process those data on a portable device or removable media. Any such request shall comply with the University portable devices and removable media acceptable use policy.

1. Describe the data which are being transferred.

2. Specify why such a transfer is necessary

3. Identify the device or removable media onto which the data are being transferred. Be specific about the name, model and asset number, if any, of the device.

4. Specify the time period for which the transfer will be necessary.

5. Identify the asset owner of the data

I confirm that it is necessary for a University business purpose to make this transfer for the time period specified, that I have the permission of the asset owner to do so and that the data are proportionate to purpose and where possible have been minimized. I will comply with the University portable devices and removable media acceptable use policy, including ensuring the encryption of the device or media. I understand that it is my responsibility to assess and mitigate the risks involved and that I will be responsible for the security of the data.

Signed Department

Print Name

Head of Department Authorisation: I authorise the transfer of the data

Signed Faculty/Directorate/Department

Print Name

NOTE: A copy of this form as signed should be sent to Head of Administration, OBIS