Mobile Computing & Remote Access Policy v1.0

Organisation	Oxford Brookes University
Title	Mobile Computing & Remote Access Policy
Creator	Gareth Packham - Head of Information Security Management
Approvals Required	1. Information Security Working Group 2. CIO
Version	Version 1.0
Owner	IT Services Information Security Working Group
Subject	The formal, approved, Mobile Computing and Remote Access policy of Oxford Brookes University
Review date and responsibility	Annually by the Head of Information Security Management

Revision History			
Date	Author	Version Number	Comments
29/03/19	Gareth Packham	0.1 (draft)	Original draft
31/03/19	Gareth Packham	1.0 (live)	Minor revisions only

1 Introduction and Policy Objectives

1.1 This document specifies the University policy for the use, management and security of any mobile computing devices ('mobile device/s') that may hold University data.

1.2 This policy applies to both mobile devices issued and owned by Oxford Brookes and personally owned mobile devices (also known as 'BYOD').

1.3 This policy also stipulates requirements for remote access to secure University systems, whether by mobile or non-mobile computing devices.

1.3 The policy applies to all users (staff, associates, consultants, contractors and visitors) who have been given access to Brookes' information and communication systems or information assets (herein 'users'). This policy only applies to students that are carrying out an official function on behalf of the University.

2 Definitions

2.1 Mobile devices that may hold University data include, but are not limited to:

- Laptop computers and netbooks
- Tablets
- Smartphones
- Portable storage devices (e.g. external hard drives, USB 'thumb drives' and memory cards).

2.2 University 'issued and owned' devices includes any device purchased, owned or leased by the University regardless of the source of funding.

2.3 Remote access refers to the ability of a user to directly access a Brookes' computer, information and communication system or information asset from an offsite or other, non-secure, location.

3 Mobile Device Policy - Technical Requirements

3.1 IT Services is responsible for determining minimum security requirements for mobile devices. Minimum security requirements will be communicated to users through advice given by IT Services staff and published guidance, in particular the *Information Handling Guidelines*.

3.2 Mobile devices shall be updated in accordance with vendor recommendations and only use operating systems supported by the vendor.

3.3 Mobile devices must store all user-saved passwords in encrypted form.

3.4 'Jailbreaking[1]' or 'rooting[1]' of University owned mobile devices is strictly forbidden. Personally owned devices that are 'jailbroken' or 'rooted' must not be used to access University systems or store University data.

4. Mobile Device Policy - User Responsibilities

4.1 Users are responsible for ensuring appropriate physical security controls are applied. These may include, but are not limited to:

- Logical 'locking' of unattended mobile devices (with a PIN, password or bitometric ID required to unlock the device).
- Secure physical storage of devices when not in use, e.g. in locked cupboards, drawers or cabinets.
- Care should be taken when travelling with mobile devices, e.g. not leaving devices unattended when offsite and keeping devices locked in the the boot of a car.

4.2 Users must report any lost or stolen mobile devices to IT Service immediately. Users must also notify IT Services if they have reason to believe a mobile device has been compromised or tampered with.

4.3 Users must ensure the use of mobile devices is in accordance with the Brookes' IT Acceptable Use Policy.

4.4 Applications must only be installed from official vendor platforms ('app stores'). Users must not install applications from untrusted sources without prior approval from IT Services.

4.5 Users must ensure devices receive updates and security patches according to vendor recommendations.

4.6 Users must consider the risk of storing or accessing University data using mobile devices. The storage of confidential University data on mobile devices is not recommended unless enhanced security controls are applied, e.g. device encryption. For restricted or confidential data users should seek advice from IT Services and subsequent approval from line management and / or appropriate data owners.

[1] To 'jailbreak' or 'root' a mobile device is to remove the limitations imposed by the manufacturer. This gives direct access to the devices operating system and increases the risk of compromise by malicious software or

agents.

4.7 Users shall take care when using personally owned mobile devices to ensure that University data is not stored or shared using personal accounts. Such usage may constitute an information security incident or breach of the Data Protection Act 2018 and should be reported to IT Services immediately.

4.8 Users must delete University data from mobile devices (whether University owned or personally owned) when the data is no longer needed for business purposes.

4.9 When users leave the University mobile devices owned by the University must be returned to IT Services (this may be via line management or other channel depending on local procedure). IT Services are responsible for either wiping and re-imaging devices for subsequent use or arranging secure collection and disposal.

4.10 When leaving the University it is the responsibility of users to ensure all University data is deleted from personally owned mobile devices (after transferring any necessary data to University-managed systems) and that tools or applications that access University systems are removed or reset. Users should be aware that inappropriate access to University data or systems after termination of employment could constitute a criminal offence.

5. Remote Access Policy

5.1 Users must only use remote access tools and solutions installed or approved by IT Services.

5.2 Remote access to University systems provided to third party suppliers and contractors must comply with the requirements of the Brookes' Network Security Policy.

5.3 IT Services and / or relevant information asset owners reserve the right to refuse remote access to University systems at their discretion.

6. Policy Enforcement

6.1 Non-compliance with this policy could result in the initiation of disciplinary procedures

against users. Under certain circumstances, failure to comply with this policy may constitute a criminal offence under the Computer Misuse Act 1990 and / or the Data Protection Act 2018.

6.2 Non-compliance with this policy by contractors or third-party suppliers may constitute a breach of contract.

6.3 Users must provide reasonable cooperation with IT Services to enable access, inspection and other appropriate actions in relation to their University owned mobile devices.

6.4 In the event of a high-severity security or data protection incident IT Services may request access to personally owned mobile devices, especially where:

- The mobile device is believed to have caused the incident
- The mobile device is believed to either store University data or has been used to access University data.

7. Related Policies & Guidance

7.1 Related policies include, but are not limited to the following University policies and guidance documents:

- IT Acceptable Use Policy
- Data Protection & Privacy Policy
- Network Security Policy
- Information Classification Policy
- Information Handling Guidelines
- Disciplinary Policy

7.2 The main IT Services contact for users will be the IT Service Desk. The IT Service Desk can be contacted:

- by telephone - 01865 483311 (or 3311 internally)
- using the self-service portal - https://service.brookes.ac.uk

7.3 The IT Services Information Security team may be contacted directly at info.sec@brookes.ac.uk