MOBILE DEVICE MANAGEMENT POLICY

1. Purpose and Scope

Whilst it is recognised that the use of mobile devices brings many benefits to the University, such devices pose a security risk as they are typically used in spaces that are susceptible to loss or theft.

This document forms the University of Reading's *Mobile Device Management Policy* which supports the *Information Security Policy*. Complying with the policy will ensure that consistent and appropriate controls are applied to University owned mobile devices to help mitigate the risks associated with their use.

1.1 The aim of the Policy is to ensure that University data on mobile devices is properly protected from unauthorised access, dissemination, alteration or deletion.

1.2 This policy applies to all staff including third parties (contractors, agency workers, students and associates) that have been issued with a University owned mobile device.

1.3 The policy applies to the use of mobile devices (laptops, mobile phones/smartphones and tablets) regardless of location, both during and outside of office hours.

1.4 Personally owned devices are out of scope of this policy. See the *Bring Your Own Device (BYOD) Policy* for information on the use of personally owned devices to process University data.

2. Responsibility

2.1 University staff issued with a University of Reading owned mobile device shall:

- Read, understand and comply with this and other related policies.
- Ensure that the device and University information stored/accessible from it remains secure. All reasonable precautions should be taken to protect devices from unauthorised physical access, loss, tampering and theft. Devices must not be left unattended in public areas.
- Use strong passwords:
  - The longer it is, the stronger it becomes and the harder it becomes to hack. Consider using a passphrase or a sequence of three random words.
  - Do not reuse passwords on other accounts, or share them.
  - Use a password manager to help you remember passwords.
  - See the University's Cyber Security webpages for more information: https://www.reading.ac.uk/internal/its/cybersecurity/passwords.aspx

- Lock your device: Use biometrics (such as a fingerprint or facial recognition), a password, a pin, or a drawn pattern.
- Ensure that security measures put in place on devices are never disabled or bypassed.
- Ensure software updates and patches are installed as soon as practicable to do so to help ensure your device remains compliant. It is the responsibility of the user to ensure that all software installed on the device remains patched and up-to-date.
- Use the University's central and secure shared drives to store and access personal and sensitive University data. See the University's *Encryption Policy* for more information.
- Report lost or stolen devices (see 4.16 and 4.17 below for more information).

2.2 Digital Technology Services (DTS) shall (where possible):

- Enrol all applicable University owned mobile devices into approved and centrally managed mobile device management solution/s.
- Ensure that users are aware of their responsibilities.
- Provide timely advice on software and operating system updates and patches via IT webpages (https://itsstatus.reading.ac.uk/).
- Maintain an asset register of all mobile devices.
- Configure devices to enable DTS to:
  - Reset device password.
  - Remotely lock or wipe (permanently erases all data on the device) a smartphone or tablet via the approved mobile device management solution.
  - Enable encryption.
  - Manage updates/patching for University of Reading approved software/applications.
  - Remove access to organisational resources if a device becomes non-compliant.

3. Consequences of Non-Compliance

3.1 Failure to comply with this policy may result in:

- Revocation of access to University systems.
- Removal of user rights to University issued mobile devices.
- Cost of replacing equipment charged to relevant department/school.
- Action taken against members of staff (including third parties) up to and including dismissal/termination of the engagement.

3.2 Suspected or actual breach of this policy or misuse of mobile devices should be reported to the IT Service Desk.

4. Policy

4.1 University owned devices are and shall remain the property of the University.

4.2 Mobile devices shall be linked to a member of staff who shall be accountable for the device.

4.3 Loan/issue records, where applicable, shall be used and kept up-to-date and accurate.

4.4 All University owned mobile devices shall (where possible) be enrolled in the centrally managed mobile device management solution/s.

4.5 The University reserves the right to prevent any device access to the University network or its services if it is considered a risk.

4.6 Mobile devices shall be encrypted where possible and appropriate to do so.

- All Windows 10 devices will be encrypted by DTS.

4.7 University approved authentication methods shall be used on all mobile devices. Passwords shall be set and managed in accordance with the University's *Password Policy*.

4.8 Automatic lock outs shall be enabled when IT equipment is left unattended.

4.9 Rooted or jailbroken devices are not permitted to connect to University IT facilities.

4.10 If additional software is required then it must be downloaded via official, authorised sources e.g. the University's Software Store (http://softwarestore.reading.ac.uk/), Google Play Store, Apple App Store etc. See the University's *Software Usage and Control Policy* for more information.

4.11 Device software (operating system, applications, anti-virus etc.) shall be kept up to date. See the University's *Patch Management Policy* for more information.

4.12 Any exception to this policy must be authorised by a member of the DTS Directorate.

Leaver/Change of Mobile Device

4.13 When devices are being transferred to another user they shall be returned to DTS to be re-imaged and re-issued to an authorised recipient within the same school/function.

4.14 Devices that are no longer needed shall be securely disposed of as per the *IT Equipment Disposal Policy*. The school/function shall notify DTS when devices are disposed of so that the associated record/s can be updated in the asset register.

4.15 If devices are not returned in a timely manner when a user leaves the University then the user's manager and Head of School/Function shall be notified. Further escalation shall result in the HR department being notified and in some cases the matter may be passed to the police for consideration.

Loss or Theft

Users of University owned devices that are lost or stolen must promptly complete the following steps:

4.16 Complete and submit the Information Security Incident Reporting Form to the Information Management and Policy Services (IMPS) team (for more information see the *Information Security Incident Response Policy*) and call DTS on 0118 378 6262 who will advise on next steps. In some cases it may be possible to remotely lock or wipe the device. Wiping the device will ensure that University of Reading data that resides on or that is accessible from the mobile device is secured.

4.17 Change University network login password and any other passwords that may have been used on the device (if DTS resets the user's network credentials on the user's behalf, ensure that the user is made aware).

5. Related policies, procedures, guidelines or regulations

This policy sits beneath the University of Reading's overarching *Information Security Policy*. This and other supporting policies can be found here:

http://www.reading.ac.uk/internal/imps/policiesdocs/imps-policies.aspx

Document control

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
1.0	N/A	DTS	Biennially	University Policy Group	May 20	May 20	May22