Device Management Policy

1 Purpose

1.1 This document forms the University of Reading's 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 devices to help mitigate the risks associated with their use. The aim of the Policy is to ensure that University data on University devices is properly protected from unauthorised access, dissemination, alteration or deletion and to ensure devices are compliant with the University's cyber security standards.

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 device.

1.3 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 Definitions

BYOD	Bring Your Own Device – the use of personally owned devices to undertake University work or to process University Data.
Device	A laptop computer, desktop computer, tablet or smartphone that is used to collect, store, access, transmit, carry, use or hold any University data.
Personally-owned devices	Devices owned, rented or leased by a member of staff.
Processing data	Obtaining, recording, holding, sharing, and retaining and deleting of University data.
Staff	Includes: • Employees (including temporary or short-term workers) of the University or a subsidiary company of the University • Volunteers, interns and those undertaking placements or work experience • Contractors engaged by the University. Students working for and/or on behalf of the University, including Post Graduate Research students

	• Those with University accounts by virtue of a visiting or courtesy title conferred by the University • Any other individual who is working on behalf of the University if they are processing University data or information

3 Roles & Responsibilities

University's Cyber & Information Security Group	Implementation, monitoring and review of this policy.
Information Management and Policy Services (IMPS)	Ensuring training, guidance and advice regarding data protection compliance is made available to staff.
Digital Technology Services (DTS)	Ensuring advice and guidance on technical specifications, such as encryption - required under this policy - is made available to staff.
Heads of Schools and Directorates	Ensuring that their staff are made aware of this policy and that breaches of it are dealt with appropriately.
University staff	Complying with this policy.

4 Consequences of Non-compliance

4.1 Failure to comply with this policy may result in us revoking your access to the University's systems, whether through a device or otherwise. It may also result in disciplinary action being taken against members of staff up to and including dismissal. In the case of breach of this policy by a contractor, worker or volunteer, it may lead to the termination of the engagement. This will apply whether the breach occurs during or outside normal working hours and whether or not use of the device takes place at your normal place of work. You are required to co-operate with any investigation into a suspected breach, which may include providing us with access to the device.

5 Guidance and Key Principles

5.1 The University is bound by the General Data Protection Regulation (the GDPR) and the Data Protection Act 2018 (the DPA). The seventh principle the DPA states that:

> "appropriate technical and organisational measures shall be taken against accidental loss or destruction of, or damage to, personal data"

5.2 Loss of devices holding University data may cause damage and distress to those who entrust us to look after their data, damage the University's reputation and its relationship with its stakeholders (including research funders), and have significant

legal and financial consequences. The Information Commissioner can impose serious monetary penalties on the University for breaches of the GDPR and DPA.

5.3 Loss of devices containing other University data may give rise to loss of rights in intellectual property, inability to register rights in intellectual property and breach of contractual and other obligations to third parties for disseminating or otherwise failing to protect confidential information.

5.4 University devices should be managed to ensure compliance with the University's cyber security standards. Devices that cannot be managed will be treated as BYOD devices unless an exemption has been registered and approved by DTS.

6 Requirements

6.1 The selection, purchase, deployment, re-use and recycling of University devices is subject to the University's **Device Policy**.

6.2 All University issued devices will be registered with an endpoint management system unless an exemption is approved by DTS.

6.3 The endpoint management system should be used to enable the following capabilities:

i) Initiate a remote lock or wipe

ii) Ensure drives are encrypted

iii) Manage updates/patching for UoR approved software/applications

iv) Remove access to UoR resources if a device becomes non-compliant

6.4 All University issued devices will be onboarded to the security systems that are managed by DTS unless an exemption is approved by DTS.

6.5 DTS reserve the right to install additional agents to permit the monitoring of compliance of University devices.

6.6 All University devices must have operating system updates applied in accordance with the **Patch Management Policy**.

6.7 All software installed on University devices must be compliant with the **Software Usage and Control Policy**.

6.8 Local administrator accounts are not normally available for users. Staff requiring administrator access must apply for this access giving a business justification. Such access is granted via a secondary account and this must be used only when required for specific activities (e.g. installing software) to reduce the risk associated with administrator access.

6.9 When devices are being transferred to another user they must be returned promptly to DTS for re-use or disposal as detailed in the University's **Device Policy**.

6.10 Users of University owned devices that are lost, stolen or damaged must promptly report this to DTS following the steps detailed in the University's **Device Policy**.

7 Related Policies, Procedures, Guidelines or Regulations

Key related policies and rules:

- Data Protection Policy
- Information Security Policy
- Regulations for the Use of the University of Reading's IT Facilities and Systems
- Encryption Policy (the Policy on Processing Personal Data and Sensitive Information off Campus or on an External Network)
- Remote and Mobile Working Policy
- Mobile Device Management Policy
- Guidance on Remote Working
- Policy on the Acquisition, Use and Transfer of Mobile Telephones
- IT Equipment Disposal Policy
- Information Security Incident Response Policy

8 Review

8.1 This Policy shall be reviewed at regular intervals and documented within the version history. Reviews will take place as a minimum at the documented frequency and in the event of any of the below:

- Significant change in University operations
- Significant change in legislation, regulatory requirements, industry guidance or similar
- In the event of a compromise of data protection or security where the content or compliance with this policy is identified as an aggravating or mitigating factor
- Any other identified requirement necessitating substantive changes ahead of scheduled review

8.2 Substantive changes shall be reviewed and approved by the Approving Authority as detailed within Document Control.

8.3 Non-substantive, minor, or administrative changes may be made by the Policy Owner, or representative of the Policy Owner, as detailed within Document control.

9 Policies Superseded by This Policy

Mobile Device Management Policy version 1.0.

10 Document control

Version	Changes	Keeper	Reviewed	Approving Authority	Next Review
1.0	First version	DTS	May 20	CUPP	May 22
2.0	• Policy name changed from Mobile Device	DTS	Dec 25	CUPP	Dec 27

	Management Policy to Device Management Policy • UoR provided devices must be managed unless valid business case • Unmanaged devices will be treated as BYOD unless exemption has been approved by DTS • All UoR issued devices will be registered with an endpoint management system unless an exemption has been approved by DTS • All University issued devices will be onboarded to the security systems managed by DTS unless an exemption is approved by DTS • DTS reserve the right to install additional agents to permit the monitoring of compliance of UoR devices	