Information Management and Policy Services (IMPS) and Digital Technology Services (DTS)

Bring Your Own Device (BYOD) Policy

1 Purpose

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

1.2 This policy applies to all University staff including third parties (contractors, agency workers, students and associates) that process University data on personally owned devices and covers computers and mobile devices (phones and tablets).

1.3 The aim of the policy is to ensure that the University complies with data protection legislation and that University information, particularly personal and sensitive information, is protected from unauthorised access, dissemination, alteration, or deletion. It complements and supports the existing Data Protection Policy and Guidelines and Regulations for the Use of the University of Reading's IT Facilities and Systems.

1.4 The policy also aims to ensure that University data, which may be data about the University, its staff, students, clients, suppliers and other business connections; information that is confidential (including but not limited to that subject to contractual obligations to maintain confidentiality), proprietary or private information; and intellectual property owned by the University or in which the University has a legal interest (in accordance with the Code of Practice on Intellectual Property), is properly protected.

1.5 Whilst it is recognised that staff use of personally owned devices for work purposes brings benefits to the University, such devices pose a high security risk to the University as they are not managed by the University, may not be patched or running adequate anti-virus software, and are likely to be more vulnerable to unauthorised access. Staff are also more likely to have admin rights on their personally owned computer which increases the risks from malware.

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.

High Risk Data	Defined in the University's Encryption Policy (see Section 7 – High risk personal data or sensitive information) and including any other information which is identified as being of a confidential or proprietary nature.
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	University staff are responsible for: • Complying with this policy. • Ensuring that their use of personally owned devices is in line with University requirements to ensure data security and the protection of University owned intellectual property and confidential information.

	• Ensuring that no unauthorised persons are able to access University owned data on their personally owned devices. • Ensuring that University data is removed from the device before disposing of the device or selling it or passing onto another individual.

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 University data and services should be accessed from University provided and managed devices wherever possible.

5.2 University data should not be stored on personally owned devices. Copying University data to personally owned devices reduces the ability for the University to know where University data is stored and makes it harder to comply with relevant legislation.

5.3 The use of unmanaged personally owned devices to access and process University data may be prohibited by contracts or agreements in place between the University and third parties. One example is the Cyber Essentials accreditation required by some schools which brings additional requirements on the management of the device and the data being processed.

5.4 The contents of our systems and University data remain University property. All materials, data, communications and information, including but not limited to, e-mail (both outgoing and incoming), telephone conversations and voicemail recordings, instant messages and Internet and social media postings and activities, created on, transmitted to, received or printed from, or stored or recorded on a device during the course of your work for the University or on its behalf is the property of the University, regardless of who owns the device.

5.5 University data held on personally owned devices is subject to the Freedom of Information Act and Data Subject Access rights under the GDPR and the DPA and must be provided to IMPS on request.

6 Requirements

6.1 If it is not possible to access University data and services from a University-provided and managed device then University data and services should be accessed using a

University approved web interface (e.g. the online versions of Microsoft Office, Outlook on the Web, the web interfaces to OneDrive for Business, web access to University systems like Employee Self-Service, Purchase to Pay etc.).

6.2 Staff access to University email and Teams on phones and tablets is permitted via the Outlook and Teams apps for iOS and Android.

6.3 University data should only be downloaded to personally owned devices if the above options are not possible.

6.4 Where the master copy of a record is held in an electronic form, it should be stored on University approved servers or services. In identifying master copies of record, staff should seek advice from their IMPS contact. Microsoft 365 (which includes OneDrive for Business and Microsoft Teams) is an approved and secure facility available to staff.

6.5 Do not use non-authorised third-party hosting services (e.g. Dropbox or Google Drive) when processing High Risk Data. Microsoft 365 is the approved and secure third-party facility available to staff.

6.6 Use the authorised remote access facilities to corporate systems (e.g. Purchase to Pay and Employee Self-service) that are both secure and encrypted to access High Risk Data on the central servers instead of transporting it on mobile devices and portable media.

6.7 Processing of personal or High Risk Data:

i. Do not process personal data or High Risk Data on personally owned devices unless this is unavoidable and absolutely necessary and has been agreed in advance with your line manager. University authorised file storage services must be used to store and access High Risk Data; this ensures that only authorised users have access to it. Do not make local copies.

ii. If you are using a personally owned device for storing High Risk Data it must be encrypted. Seek advice from DTS if you are unsure how to do this. We recommend you bear in mind the requirements of this policy when purchasing a device you wish to use for work purposes.

iii. If processing High Risk Data is necessary, then consider whether data can be anonymised to obscure the identity of the individuals concerned. Further guidance on anonymisation can be found at https://ukdataservice.ac.uk/media/622417/managingsharing.pdf.

iv. Do not process or view High Risk Data in public places where you can be overseen.

v. Use the University's VPN if you need to process High Risk Data whilst connected to a public Wi-Fi service.

vi. The loss or theft of a personal device that holds personal or High Risk Data must be reported immediately in accordance with the University Security Incident Response Policy and Procedures.

6.8 Managing your device:

i. Anyone using personally owned devices to store or process University data should also follow the advice and guidance provided in www.reading.ac.uk/digital-

technology-services/cyber-security to ensure that the devices are as secure as possible (e.g. software is up to date and security updates have been applied).

ii. Control access to the device via touch ID, face ID, password or PIN. Passwords must meet the University's password requirements.

iii. Use a screen or device lock that will trigger after a short period of inactivity (no longer than 10 minutes) and manually lock the screen when you walk away from the device

iv. Configure your device to enable you to remote-wipe it should it be lost or stolen.

6.9 When data is encrypted by the user, a procedure for the management of electronic encryption keys must be established to ensure the adoption of best practice guidelines and compliance with both legal and contractual requirements and to ensure information can be accessed by authorised users when needed.

6.10 When transmitting encrypted data to/from countries outside the UK, the encryption used must meet the regulatory requirements of both countries. If the other country does not permit encryption then high-risk data must not be transmitted to that country.

6.11 The University reserves the right to prevent access to the University network or services by any device that is considered a risk.

6.12 Do not keep any information longer than is necessary and only in line with University Record Retention guidelines. Avoid duplication of information wherever possible.

6.13 Any use of a personal device for or in connection with University work must be carried out in accordance with the University's procedures relating to equal opportunities, harassment, safeguarding, the Prevent duty, use of social media, intellectual property and with any relevant laws.

6.14 You must pay for your own device costs under this policy, including but not limited to voice and data usage charges and any purchase and repair costs. By using your device for University related purposes and unless otherwise agreed with you in a separate agreement with the University, you acknowledge that you alone are responsible for all costs associated with the device and that you understand that your business usage of the device may increase your voice and data usage charges.

6.15 Personally owned devices are not permitted to connect to the University wired network or staff Wi-Fi network. They can connect to the eduroam network for Internet access only. Personally owned devices connected to eduroam will be treated as untrusted devices in terms of access to University services and digital products.

6.16 On leaving the University, ensure all University data is deleted securely from your device. Ensure that master copies of documents that are required by the University are transferred to other University staff before you leave.

6.17 Remove University data from the device before disposing of the device or selling it or passing onto another individual. Ideally, the device should be reset to factory defaults.

6.18 Do not leave your device unattended in situations where others could access it and ensure it is physically secure at all times.

6.19 The loss or theft of a personal device that holds any other University data, or where you believe that the device may have been accessed by an unauthorised person or otherwise compromised, must be reported as soon as possible to IMPS.

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)
- Classification Policy
- 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
- Code of Practice on Intellectual Property
- Equal Opportunities
- 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

Bring Your Own Device Policy version 1.3 (issued 2022).

10 Document Control

Version	Changes	Keeper	Reviewed	Approving Authority	Next Review
1.0	Legislation and DTS Updates	IMPS	May 17	IMPS	Jul 18
1.1		IMPS	Oct 19	IMPS	Nov 20
1.2		IMPS	Apr 21	RMG	Aug 22
1.3	Review period updated	IMPS	Aug 22	CUPP	Aug 24
1.4	• UoR data and services should be accessed from UoR managed devices • Use of BYOD may be prohibited by specific contracts or agreements • UoR data held on BYOD is subject to the Freedom of Information Act and Data Subject Requests • Revised the requirements for processing of High Risk Data on BYOD	IMPS/DTS	Dec 25	CUPP	Dec 27