Bring Your Own Device (BYOD) Policy

1. Purpose

This policy applies to all University staff that process University data on personally owned devices.

1.1 This document sets out the University's policy on the use of personally owned devices to process University data and forms part of the University's Information Security Policy.

1
legislation and that University information, in particular 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 ICT 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

- 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.

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.

- 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 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"

Loss of devices holding University data may cause damage and distress to those who entrust us to look after their data, damage the Uni.2 (g9.7 (u)-p2.3 (k)10.3 (ua h)-4.6 (o)-2.6 (ai)3 (,)16 (t

- Keep your device's software up to date. This includes operating systems, applications, and anti-virus and malware protections.
- Personally owned devices can only be connected to the University's Guest Network (e.g. the Eduroam WiFi service) when used on campus. IT will not register personally owned devices for connection to the wired campus network.
- Do not use public WiFi spots if you are using a personally owned device for High Risk Data. Disable Bluetooth and WiFi if they are not needed
- 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.
- 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.
- Do not leave your device unattended in situations where others could access it and ensure it is physically secure at all times. Security cables, such as Kensington locks, should be used to secure laptops when they are used in open access areas and offices. If

- If processing High Risk Data is necessary, then consider anonymising the information to obscure the identity of the individuals concerned. Further guidance on anonymisation can be found at http://www.data-archive.ac.uk/create-manage/consent-ethics/anonymisation.
- Consider instead using a University authorised file storage services to store and access High Risk Data; this ensures that only authorised users have access to it
- 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. Office 365 is an approved and secure facility available to staff.
- Do not use non-authorised third party hosting services (e.g. Dropbox or Google Drive) when processing High Risk Data. Office 365 is the approved and secure third-party facility available to staff.
- 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
- If you are sending High Risk Data by email to addresses external to the University ensure that you do this in accordance with the Encryption Policy. Where a University issued email account has been provided, personal email addresses should not be used unless in exceptional circumstances. Data sent external to the University should be sent to organisation or.6 (al)-3.1 (r

- 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.
- 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.

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 Working Policy
- 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

Policies superseded by this policy

Not applicable

Document control