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

University of Reading

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**.

1.2 Whilst it is recognised that staff use of personally owned devices for work purposes brings many benefits to the University, such devices pose a high security risk if they are left vulnerable to theft, loss and unauthorised access.

1.3 The aim of the policy is to ensure that the University complies with data protection 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 DTS 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 Some devices may not have the capability to connect to our systems. We are not under any obligation to modify our systems or otherwise assist Staff in connecting to our systems.

2. Definitions

Processing data	means obtaining, recording, holding, sharing, and retaining and deleting of University data.
BYOD	Bring Your Own Device – the use of personally owned devices to undertake University work or to process University Data.
Personally owned devices	Includes - but is not limited to – laptops, personal computers, netbooks, tablets and smartphones that are used to collect, store, access, transmit, carry, use or hold any University data. It applies to the use of the Personally Owned Device both during and outside of normal working hours and whether or not it is used at your normal place of work.
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.

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.

3. Roles & Responsibilities

University's 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 Department (DTS)	Ensuring advice and guidance on technical specifications, such as encryption - required under this policy - is made available to staff.
Heads of Schools, Functions and Departments	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. - 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 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 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.

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.

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. Requirements

- Control access to the device (use fingerprint scanning if available, otherwise by password or PIN if neither fingerprint nor password is possible). Passwords must meet the University's minimum password requirements (details available on IT Help and Support/PC Security webpages).
- Use a screen or device lock that will trigger after a short period of inactivity (no longer than 10 minutes).
- Configure your device to enable you to remote-wipe it should it be lost or stolen[1].
- 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.

[1] If your device is configured to connect to Office365 it can be remote wiped by IT.

- 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 Wi-Fi service) when used on campus. IT will not register personally owned devices for connection to the wired campus network.
- Do not use public Wi-Fi spots if you are using a personally owned device for High Risk Data. Disable Bluetooth and Wi-Fi 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 used in open access areas and offices. If you are using a personal device for High Risk Data, do not share your device with others, including members of your household.
- 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.
- 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.

6. Guidance and Key Principles

The following key principles underpin this policy statement. All staff must comply with these principles.

- 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.
- 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.
- Avoid processing personal data on personally owned devices whenever possible and do not use personally owned equipment to process High Risk Data unless this is unavoidable and absolutely necessary and has been agreed in advance with your line manager.

- 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 company issued email accounts, and not to personally owned accounts, unless the externally owned account is the only available method of contact, for example in the case of a sole trader or contractor. In all cases the address must be verified and checked prior to sending.
- Do not process or view High Risk Data in public places.
- 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.
- When transmitting encrypted data to/from countries outside the UK, have regard for the regulatory regime in the other country. You may be asked to provide passwords and/or encryption keys.
- The University reserves the right to prevent access to the University network or services by any device that is considered a risk. In exceptional circumstances the University may require access to University information on a personally owned device or require that data on a personally owned device be remotely wiped (e.g. in the event of loss or theft of the device).
- Do not keep any information longer than is necessary and only in line with University Record Retention guidelines. Avoid duplication of information wherever possible.
- Anyone using personally owned devices to store or process University data should also follow the advice and guidance provided in www.reading.ac.uk/cybersecurity to ensure that the devices are as secure as possible (e.g. software is up to date and security updates have been applied).

- 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

VERSION	SECTION	KEEPER	REVIEWED	APPROVING AUTHORITY	APPROVAL DATE	START DATE	NEXT REVIEW
1.0		IMPS	MAY 17	UEB	MAY 17	JULY 17	JULY 18
1.1	Legislation and DTS Updates	IMPS	OCT 19	IMPS	OCT 19	NOV 19	NOV 20