1. Use Your Own Device (UYOD) Policy

RADA (which includes RADA Business) recognises that students, employees and contractors (Users) may use their own smartphones, tablets and laptops to work or study in a way that suits them.

This policy is intended to protect the security and integrity of RADA's data and technology infrastructure. Limited exceptions to the policy may occur due to variations in devices and platforms and RADA reserves the right to request any User cease using a particular device if it will harm the security or integrity of organisation's infrastructure.

It is critical that RADA's data and technology infrastructure is protected and therefore, Users must agree to follow the standards and procedures in this policy to be able to connect their devices to the company network or receive company information on it. This policy puts the emphasis on the user to make sure that their own devices are secure. RADA expects these requirements will be observed so that the further implementation of direct restrictions or control of User's devices is avoided.

2. Acceptable Use

2.1. The company defines acceptable business use as activities that directly or indirectly support RADA's activities. See the 'Use of telephones, IT, Storage, Internet and email policy' in the staff handbook and 'Internet, WiFi and email usage' in the student handbook.

2.2. Users may use their own device to access the following resources: Office 365, including email, calendars, contacts, documents and Teams and Dynamics, Sharepoint, CRM (including Scheduler), Zoom and Sage according to the requirements of their role.

3. Devices and Support

3.1. Smartphones, tablets, laptops and personal computers may be used to connect to the network or access RADA services such as Sharepoint or Office 365 **provided that**:

- Device Software & Applications
    - All software not required by the User is removed
    - All software that is no longer supported for security updates or licenced is removed
    - Only use Microsoft applications (apart from browsers, Sage, UC-One/Webex and Zoom) for RADA data
    - Only use internet browsers to access RADA data which are up to date versions of Microsoft Edge, Mozilla Firefox, Google Chrome and Apple Safari but **not** Windows 10 Mobile or Chrome OS.

- User Accounts
    - All User accounts not in use are removed from the device
    - User accounts used for processing RADA data must not be local admins
    - Only the individual employee, contractor or student should be able to access the device. If a device (such as a home computer) is used by others (such as family members), each user of that device must have an individual account on the device that is
        - password protected
        - set to lock itself with a password or PIN if it is idle for five minutes

        - set to lock automatically if an incorrect password is entered after several attempts

- Device Security
    - All devices have built in firewalls enabled at all times
    - Auto run when connection media such as USB devices is disabled

- Antivirus
    - Up to date anti-virus and anti-malware software is in place (such as https://www.sophos.com/en-us/products/free-tools.aspx)

- Updates and software versions
    - devices and applications are kept up to date and auto-update for security patches is enabled.
    - Devices using Windows 10 Mobile or ChromeOS are not used.
    - The device is using a supported operating system (see list below):

Supported operating systems

	Supported
Mobile	Android 10 or later iOS 12 or later
Desktop/Laptop	Windows 10, update 20H2 or later Catalina 10.15 or later

3.2. Connectivity issues are supported by IT; Users should contact the device manufacturer or their carrier for operating system or hardware-related issues.

4. Security

4.1. In order to prevent unauthorized access, devices must be password protected using the features of the device and a strong password is required to access the company network. This includes using biometric authentication such as fingerprint and face recognition.

4.2. Users' access to company data is limited based on user profiles as required for their role, implemented by IT and automatically enforced.

4.3. The User's device may be remotely wiped without notice if

- **the device is lost, or**
- **the User terminates their employment (or contract or ceases to be a student), or**
- **IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.**

5. Data Protection

5.1. Cooperation with subject access requests

Any individual whose personal date is held by the Company has the right to make a subject access request. Consequently, the Company may have to access your device to retrieve any data that is held on it about an individual. You must allow the Company to do this. Access to your device will only be for the purposes of fulfilling the subject

access request. Data which is not relevant to the request will not be removed and access limited to it to the extent necessary. Any request for access to personal devices will be signed off by the Director of Finance & Operations.

5.2. Retention of Personal or Commercial Data
Users must not keep personal or other business data for longer than necessary for the purpose for which it is being used, unless there is a requirement to retain it for longer to comply with a legal obligation.

5.3. Deletion of Data
Users must ensure that, if they delete information from a device, the information must be permanently deleted rather than left in the device's waste management system. If removable media, e.g. a USB drive or CD, is used to transfer personal data, Users must ensure that the personal data is deleted after the transfer is complete.

5.4. End of Employment
Prior to the last day of employment or contract or ceasing to be a student, all Users must delete work-related personal data on their own device.

6. Risks/Liabilities/Disclaimers

6.1. While IT will take every precaution to prevent the User's personal data from being lost, in the event it must remotely wipe a device, it is the User's responsibility to take additional precautions, such as backing up email, contacts, etc.

6.2. The company reserves the right to disconnect devices or disable services without notification.

6.3. Lost or stolen devices must be reported to the Helpdesk and director of Finance & Operations within 24 hours of the loss being identified. Users are responsible for notifying their mobile carrier immediately upon loss of a device.

6.4. The User is expected to use their devices in an ethical manner at all times and adhere to the company's acceptable use and social media policies.

6.5. The User is personally liable for all costs associated with their device.

6.6. The User assumes full liability for risks including, but not limited to, the partial or complete loss of company and personal data on their device due to an operating system crash, errors, bugs, viruses, malware, and/or other software or hardware failures, or programming errors that render the device unusable.

6.7. RADA reserves the right to take appropriate disciplinary action up to and including termination of contract for noncompliance with this policy.

Author	FJ
Date of Issue	10 Aug 2022
Version	2.0
Approved by	RADA DFO, RB Director of Operations
Date of next review	July 2023
Distribution list	• Cara Director • All staff via HR (Breathe) • All students via SAS (Handbook) • RB Tutors via RB DoO