Bring Your Own Device (BYOD) Policy

Pronounced80 Solutions Limited

Freeing business from the tyranny of legacy software

Version 1.0 | Effective: May 2026 | Review: Annual

1. Purpose

To set out conditions under which personally-owned devices may be used for business purposes.

2. Scope

Any personally-owned device used to access company or client systems or data.

3. Eligibility and Approval

- BYOD use is permitted only where the device meets the controls in this policy and is approved by the Director.
- Where a client prohibits BYOD or imposes stricter controls, the client requirement applies.

4. Mandatory Controls

- Device encryption enabled.
- Strong passcode / biometric unlock and automatic screen lock.
- Current, supported operating system; security updates installed promptly.
- Endpoint protection where applicable.
- MFA enabled for business accounts.

5. Data Separation

- Business data accessed only via approved apps/services (e.g. Microsoft 365 apps, browser-based access).
- Client confidential data is not stored in personal cloud accounts (iCloud, personal Google Drive, personal OneDrive, etc.).

6. Acceptable Use

- The Acceptable Use Policy applies on BYOD devices when accessing business data.

7. Lost / Stolen / Compromised Devices

- Reported immediately.
- Sessions revoked, credentials rotated and remote sign-out actioned.

8. Off-Boarding / End of Engagement

- Business accounts signed out and removed from the device.
- Any business data on the device deleted; confirmation provided where required.

9. Privacy

We do not access personal content on BYOD devices. Security actions are limited to business data and accounts.