Bring Your Own Devices (BYOD) Policy

Company Name:	JPN Training
Approver (Date):	Julia Palmer-Ndu – 28/07/2026
Review due date:	July 2027
Current Version:	1.0
Update history:	28/07/2026 Document Creation
Document Type	Operational Policy
Classification	Internal Use Only

1. Introduction

This Bring Your Own Device (BYOD) Policy defines the requirements, responsibilities, and security controls for employees and contractors who use personally owned devices to access JPN Public Training data, systems, or communication platforms. The aim is to protect company information while allowing flexible working.

2. Scope

This policy applies to:

All employees, contractors, consultants, and temporary workers.

All personal devices used to access JPN Public Training systems, including:

- Mobile phones
- Tablets
- Laptops and personal computers
- Wearables capable of storing or transmitting company data

3. Eligibility & Authorisation

- BYOD use must be approved by the line manager and the IT department.
- Devices must meet the minimum security requirements in Section 4.
- IT reserves the right to deny or revoke BYOD access at any time if security risks are identified.

4. Security Requirements for Personal Devices

To access JPN Public Training systems, personal devices must:

- Be protected with a password, PIN, fingerprint, or facial recognition.
- Have automatic screen lock enabled (max 5 minutes inactivity).
- Run supported and regularly updated operating systems.
- Have up-to-date antivirus or endpoint protection installed (where applicable).
- Not be rooted, jailbroken, or altered to bypass security controls.
- Have full-disk encryption enabled (laptops) and device encryption enabled (mobile devices).
- Use Multi-Factor Authentication (MFA) where required.

5. Acceptable Use

Employees must:

- Only access company systems through approved applications and secure login methods.
- Ensure personal devices are used responsibly and professionally when handling company information.
- Immediately report any lost, stolen, or compromised device to IT.

Keep company emails and files within approved apps (e.g., Microsoft 365) and not download them to unapproved locations.

Employees must not:

- Store sensitive company information on unapproved apps or cloud services.
- Share devices with family or friends while logged into company accounts.
- Circumvent security controls or install unapproved tools to access company data.

6. Company Rights & Device Management

- IT may install and require security tools such as mobile device management (MDM) or conditional access.
- JPN Public Training may remotely wipe company data from a personal device if:
- The device is lost or stolen.
- The user leaves the business.
- A security risk is identified.
- The user violates this policy.
- Only company data will be removed; personal content will not be accessed.

7. Data Protection & Privacy

- JPN Public Training will not access personal data such as photos, messages, contact lists, or private apps.
- Monitoring applies only to company applications, login attempts, and security controls.
- Employees are responsible for backing up personal data.

8. Offboarding & Role Changes

When an employee leaves or changes role:

- BYOD access is removed.
- Company data is wiped from the device.
- Access to Microsoft 365, CRMs, cloud services, and other systems is revoked.

9. Incident Reporting

Any suspected security incident involving a BYOD device must be reported immediately to IT, including:

- Loss or theft
- Malware infection
- Unauthorised access
- Device compromise

10. Enforcement

Violations of this policy may result in:

- Removal of BYOD access
- Disciplinary action
- Required return of company-owned data or assets

11. Review

This policy will be reviewed annually or after significant changes in technology, legislation, or business operations.