

Privacy by Mobile Device Management Policy

Gibble SaaS Platform

Prepared by: Gregory Ibbotson – G.I. IT Security

Version: 1.0



Leftorium Pty Ltd

Suite 204, 189E South Centre Road, Tullamarine VIC 3043

Email: info@gibble.com.au | Phone: (03) 9744 2887

ABN 65 7612 792

Trading as **Gibble** - gibble.com.au

Leftorium Pty Ltd (Trading as Gibble) Mobile Device Management Policy

Last updated: July 2025

Table of Contents

1.	Purpose	3
2.	Scope	3
3.	Definitions	4
4.	MDM Principles	4
5.	Mobile Device Requirements	4
6.	Device Management Procedures	5
7.	BYOD Considerations	6
8.	Monitoring and Auditing	6
9.	Incident Management	7
10.	Roles and Responsibilities	7
11.	Training	8
12.	Compliance	8
13.	Violations	8
14.	Contact Information	9

Leftorium Pty Ltd (Trading as Gibble) Mobile Device Management Policy

Last updated: July 2025

1. Purpose

1.1 This Mobile Device Management (MDM) Policy ("Policy") outlines the standards and procedures for managing mobile devices used to access the systems, platforms, and data of Leftorium Pty Ltd, trading as Gibble ("we," "us," or "our"), including our SaaS platforms for learning, payroll, student management, human resources management, and the Ready People App. The Policy ensures the security, integrity, and compliance of mobile devices to protect sensitive information, including personal information, customer data, and biometric data.

1.2 The Policy integrates with our Security Policy (Section 5.3), Access Control Policy (Section 5), Encryption Policy (Section 5), Employee and Contractor Security Policy (Section 5), and other policies, leveraging Microsoft Intune, Amazon Web Services (AWS), Microsoft Entra, and Adlumin Managed Detection and Response (MDR) services to enforce secure mobile device usage.

1.3 We are committed to compliance with applicable data protection and cybersecurity laws, including:

- Australian Privacy Principles (APPs) under the *Privacy Act 1988* (Cth), particularly APP 11.
- EU General Data Protection Regulation 2016/679 (GDPR), Article 32.
- *Privacy Act 2020* (New Zealand), Information Privacy Principle (IPP) 5.
- Singapore Personal Data Protection Act (PDPA).
- California Consumer Privacy Act (CCPA/CPRA).
- Japan Act on the Protection of Personal Information (APPI).

1.4 For inquiries, contact our Security Officer at:

- **Email:** security@gibble.com.au
- **Address:** Level 2, Suite 204, 189E South Centre Rd, Tullamarine VIC 3043, Australia
- **Phone:** +61 3 9744 2887

1.5 This Policy is reviewed annually or as needed to reflect changes in regulations, technology, or business operations. Updates are posted at www.gibble.com.au/mdm.

2. Scope

2.1 This Policy applies to:

- All mobile devices (e.g., smartphones, tablets) used by employees, contractors (e.g., in Vietnam and the Philippines for Gibble platforms), and authorised customer personnel to access Gibble's systems, platforms, or data.
- Gibble's platforms and infrastructure, including those hosted on AWS (e.g., S3, RDS, EC2), Microsoft Entra (e.g., Azure Blob Storage, Entra ID), and third-party systems (e.g., Salesforce, Stripe).
- Data processed by Gibble, including personal information (e.g., names, contact details, biometric data), customer data, and analytics data, as described in the Privacy Policy (Section 4).

Leftorium Pty Ltd (Trading as Gibble) Mobile Device Management Policy

Last updated: July 2025

- The Ready People App, which may process location-based services and timekeeping data with user consent, per the Privacy Policy (Section 19.1).

2.2 It covers both company-issued and personal devices (Bring Your Own Device, BYOD) used for work purposes, complementing the Security Policy (Section 5.3), Access Control Policy (Section 5), and Employee and Contractor Security Policy (Section 5).

3. Definitions

3.1 **Mobile Device:** Any portable device (e.g., smartphone, tablet) capable of accessing Gibble's systems or data.

3.2 **MDM Solution:** Software (e.g., Microsoft Intune) used to manage, monitor, and secure mobile devices.

3.3 **BYOD:** Bring Your Own Device, referring to personal devices used for work purposes under Gibble's management.

3.4 **Personal Information:** Information relating to an identified or identifiable individual, as defined in the Privacy Policy (Section 4).

4. MDM Principles

4.1 **Security:** Mobile devices are configured to protect sensitive data and prevent unauthorised access.

4.2 **Compliance:** Device management aligns with data protection and cybersecurity laws, including GDPR and APPs.

4.3 **Least Privilege:** Devices access only the systems and data necessary for authorised tasks, per the Access Control Policy (Section 4).

4.4 **Monitoring:** Device activities are monitored for compliance and security, per the Information Security Incident Management Policy (Section 6).

4.5 **User Accountability:** Employees and contractors are responsible for adhering to device security requirements.

5. Mobile Device Requirements

5.1 **Device Enrolment:**

- All mobile devices accessing Gibble's systems must be enrolled in Microsoft Intune, managed via Entra ID.
- Enrolment requires user authentication and acceptance of Gibble's MDM terms.
- BYOD devices are enrolled in a separate profile to segregate work and personal data, per the Privacy by Design and Default Policy (Section 6).

5.2 **Security Configurations:**

Leftorium Pty Ltd (Trading as Gibble) Mobile Device Management Policy

Last updated: July 2025

- Devices must have:
 - Strong passwords or biometric authentication (e.g., fingerprint, face recognition).
 - Full-disk encryption using AES-256, per the Encryption Policy (Section 5.1).
 - Up-to-date operating systems and security patches.
 - Endpoint protection (e.g., antivirus, anti-malware) enforced via Microsoft Intune.
- Jailbroken or rooted devices are prohibited.
- Non-compliant devices are blocked from accessing Gibble systems, per the Access Control Policy (Section 5).

5.3 Application Management:

- Only approved applications (e.g., Ready People App, Gibble platform apps) may access Gibble's systems.
- Microsoft Intune enforces application policies, including app isolation to prevent data leakage.
- Unapproved apps are blocked from accessing work data on BYOD devices.

5.4 Network Security:

- Devices must use secure connections (e.g., TLS 1.3) for data transmission, per the Encryption Policy (Section 5.2).
- Public Wi-Fi use requires a VPN (e.g., AWS Client VPN) configured by the IT Manager.
- Location-based services in the Ready People App are disabled by default, requiring explicit user consent, per the Privacy Policy (Section 19.1).

6. Device Management Procedures

6.1 Device Registration:

- Employees and contractors register devices with the IT Manager via a secure portal or it@gibble.com.au.
- Registration includes device type, OS version, and user details.
- Customer personnel devices are registered by their organisation's admin, with Gibble's approval.

6.2 Device Monitoring:

- Microsoft Intune monitors device compliance (e.g., encryption, patch status) in real-time.
- Adlumin MDR monitors device activities for anomalies (e.g., unauthorised access), per the Information Security Incident Management Policy (Section 6).
- AWS CloudTrail and Microsoft Defender for Cloud log device interactions with Gibble systems.

6.3 Remote Wipe and Lock:

- Lost or stolen devices are remotely locked or wiped via Microsoft Intune.

Leftorium Pty Ltd (Trading as Gibble) Mobile Device Management Policy

Last updated: July 2025

- BYOD devices have only work-related data wiped, preserving personal data, per the Privacy by Design and Default Policy (Section 6).
- Employees and contractors report lost/stolen devices to security@gibble.com.au within 1 hour.

6.4 Device Decommissioning:

- Upon termination or device replacement, work data is wiped, and devices are unenrolled from Intune.
- Decommissioning follows the Data Retention and Deletion Policy (Section 6) and Employee and Contractor Security Policy (Section 10).

7. BYOD Considerations

7.1 Segregation:

- Work data is isolated in a secure container on BYOD devices using Microsoft Intune's app protection policies.
- Personal data is not accessed or monitored, per the Privacy by Design and Default Policy (Section 6).

7.2 User Agreement:

- BYOD users sign an agreement acknowledging:
 - Gibble's right to manage work-related data and apps.
 - Remote wipe capabilities for work data.
 - Compliance with this Policy and the Employee and Contractor Security Policy (Section 5).

7.3 Privacy:

- Gibble does not collect personal data from BYOD devices beyond what is necessary for work purposes, per the Privacy Policy (Section 4).
- Data subjects can request access or deletion of work-related data, per the Data Subject Rights Policy (Section 5).

8. Monitoring and Auditing

8.1 Monitoring:

- Adlumin MDR and Microsoft Intune monitor device compliance and security events.
- AWS CloudTrail and Microsoft Defender for Cloud log device access to Gibble systems, per the Access Control Policy (Section 8).

8.2 Auditing:

- Quarterly audits verify device compliance with this Policy, including encryption and patch status.
- Annual ISO 27001 and SOC 2 Type II audits include MDM practices.

- Audit reports are available to customers upon request at security@gibble.com.au.

9. Incident Management

9.1 Incident Reporting:

- Suspected device-related incidents (e.g., malware, unauthorised access) are reported to security@gibble.com.au within 1 hour, per the Information Security Incident Management Policy (Section 6).
- Incidents involving personal information are escalated to the Data Breach Response Team, per the Data Breach Response Plan (Section 5).

9.2 Response:

- The Security Officer investigates incidents with Adlumin MDR support, locking or wiping affected devices as needed.
- Recovery follows the Business Continuity and Disaster Recovery Policy (Section 10).

10. Roles and Responsibilities

10.1 Security Officer:

- Oversees MDM policy implementation and compliance.
- Investigates device-related incidents with Adlumin MDR.
- Approves device configurations and exceptions.

10.2 IT Manager:

- Configures and manages Microsoft Intune for MDM.
- Registers and decommissions devices.
- Ensures device compliance with security settings.

10.3 Data Protection Officer (DPO):

- Ensures MDM practices comply with data protection laws.
- Addresses data subject inquiries related to device data (privacy@gibble.com.au).

10.4 Employees and Contractors:

- Enrol devices in Microsoft Intune and comply with this Policy.
- Report lost/stolen devices or incidents to security@gibble.com.au within 1 hour.
- Complete MDM training, per the Employee and Contractor Security Policy (Section 7).

10.5 Customers:

Leftorium Pty Ltd (Trading as Gibble) Mobile Device Management Policy

Last updated: July 2025

- Ensure their personnel's devices comply with Gibble's MDM requirements.
- Report device-related issues to their Gibble account manager or support@gibble.com.au.

11. Training

11.1 Employees and contractors, including those in Vietnam and the Philippines, receive annual training on:

- MDM policies and device security requirements.
- Safe use of the Ready People App and other Gibble applications.
- Reporting device-related incidents.

11.2 Customers receive guidance on MDM requirements during onboarding, per the Acceptable Use Policy (Section 5).

12. Compliance

12.1 This Policy aligns with:

- ISO 27001 A.12.4 (Security Monitoring) and A.12.6 (Technical Vulnerability Management).
- GDPR Article 32 (Security of Processing).
- APP 11 (Security of Personal Information).
- NIST 800-53 SC-7 (Boundary Protection).
- PDPA, CCPA/CPRA, and APPI security requirements.

12.2 AWS, Entra, and Intune compliance dashboards, supported by Adlumin MDR logs, ensure adherence to these standards.

13. Violations

13.1 Violations of this Policy (e.g., using non-enrolled devices, bypassing encryption) may result in:

- Disciplinary action for employees or contractors, per the Employee and Contractor Security Policy (Section 12).
- Immediate suspension of device access, per the Access Control Policy (Section 12).
- Contractual penalties for customers or vendors, per the Vendor Management Policy (Section 12).
- Reporting to regulators if the violation constitutes a data breach, per the Data Breach Response Plan (Section 8).

13.2 Violations are investigated by the Security Officer with Adlumin MDR support.

14. Contact Information

14.1 For MDM-related inquiries or to report issues, contact:

- Security Officer: security@gibble.com.au
- Data Protection Officer: privacy@gibble.com.au
- IT Manager: it@gibble.com.au
- Phone: +61 3 9744 2887

14.2 Complaints can be escalated to:

- **Australia:** Office of the Australian Information Commissioner, enquiries@oaic.gov.au, 1300 363 992.
- **New Zealand:** Office of the Privacy Commissioner, enquiries@privacy.org.nz.
- **EU:** Relevant supervisory authority (e.g., ICO in the UK).
- **Singapore:** Personal Data Protection Commission, info@pdpc.gov.sg.
- **USA:** Relevant state authority (e.g., California Attorney General).
- **Japan:** Personal Information Protection Commission, info@ppc.go.jp.