**Mobile Device Management (MDM) Policy**

**Purpose:** To ensure the security, integrity, and appropriate use of company data and systems accessed via employee laptops and mobile devices.

**Scope:** This policy applies to all laptops, tablets, smartphones, and other mobile devices issued by the company or used to access company resources.

**Policy Statement:**

1. **Device Management:** All employee laptops provided by the company are enrolled in the organisation’s Mobile Device Management (MDM) system. This enables centralised control, configuration, and security enforcement.
2. **Monitoring:** The company monitors device compliance with security policies, including but not limited to:
* Operating system updates and patching
* Antivirus and anti-malware status
* Encryption status
* Installation of approved software only
* Usage of VPN and secure connections
1. **Access Control:** Devices must be password protected, and the company enforces multi-factor authentication where applicable. Devices found to be non-compliant may have access to company systems restricted or revoked until compliance is restored.
2. **Data Protection:** Company data on employee devices is protected by encryption and remote wipe capabilities in the event of loss or theft. Employees must report lost or stolen devices immediately.
3. **Privacy:** While the company monitors devices to ensure security and compliance, it respects employee privacy by limiting monitoring to work-related data and activity. Personal data stored on devices is not accessed without consent unless legally required.
4. **User Responsibilities:** Employees are required to use company devices responsibly, adhere to security guidelines, and not attempt to circumvent management controls.
5. **Policy Compliance:** Violation of this policy may result in disciplinary action, up to and including termination of employment.