INTEGRITY IT SERVICES.ZW

Legal Notice & Official Privacy Policy

Headquarters: Guruve, Zimbabwe

1. Legal Notice & Terms of Service

1.1. Service Agreement

By engaging Integrity IT Services.zw ("the Company") for computer maintenance, repair, or mobile IT support, the client agrees to the terms outlined herein. The Company operates as a mobile entity, providing on-site diagnostics and repair to institutions, clinics, and private clients.

1.2. Limitation of Liability and Data Backup

> **Critical Notice:** While we treat all hardware with the utmost precision, the client is strictly responsible for backing up all sensitive data, school records, patient files, and personal information prior to any hardware or software intervention.

Integrity IT Services.zw shall not be held liable for any data loss, hardware failure, or operational downtime that occurs during or after the servicing of equipment. All services are performed at the client's own risk.

1.3. Abandoned Equipment

Any hardware or peripherals left in the custody of our technicians and not claimed within thirty (30) days of service completion will be considered abandoned and may be recycled or sold to recover labor costs.

1.4. Governing Law

These terms and conditions are governed by and construed in accordance with the laws of Zimbabwe. Any disputes relating to these terms and conditions will be subject to the exclusive jurisdiction of the courts of Zimbabwe.

2. Privacy Policy

Integrity IT Services.zw is committed to the absolute privacy and security of our clients' data. As a service provider frequently handling machines from medical clinics and educational institutions, we adhere to strict confidentiality protocols.

2.1. Data Collection

During our intake process, we collect only the information necessary to facilitate repair and maintain our service warranties. This includes:

- Institution or Client Name
- Device Make, Model, and Serial Number / Service Tag
- Physical Audit Details (noting existing cosmetic damage)
- Service History and Diagnostic Logs

2.2. Data Processing and Hardware Operations

We utilize an offline-first data infrastructure. Client intake data is stored securely on encrypted local SQLite databases deployed on our field devices. To facilitate immediate, on-site issuance of service tickets without relying on third-party cloud networks, our technicians maintain a continuous, forever-on Bluetooth configuration. This dedicated connection routes intake data directly to our portable thermal printers. This continuous operational state is strictly limited to authorized hardware pairing and does not scan, collect, or broadcast data to unauthorized networks or client systems.

2.3. Data Access and Sharing

We do not copy, browse, or transfer client files (such as documents, photos, or institutional databases) unless explicitly requested by the client for data recovery or migration purposes. Client contact and intake information is never sold, rented, or shared with third-party marketing agencies.

2.4. Data Retention

Service records, including serial numbers and labor summaries, are retained securely for accounting, warranty verification, and the scheduling of preventative maintenance. Clients may request the deletion of their personal contact data from our active service logs at any time by submitting a written request.