Privacy Policy

Last updated: 2026-09-29 · Version 2026-09-29 (updated from 2026-09-28: documented the POPIA section 72 basis for the cross-border transfer to Supabase's EU hosting — previously flagged as needing confirmation)

1. Who we are, and who's responsible for what

This policy explains how Vantic (Pty) Ltd (registration number 2026/765066/07) ("we", "us") — trading as Vantic — of 68-82 Steenloper Street, Monumentpark, Pretoria, Gauteng, South Africa, processes personal information through the Vantic platform.

Vantic acts as an "Operator" under POPIA, not the "Responsible Party." Your school, academy, or club (your "Organization") is the Responsible Party — they decide what player and staff data to enter, and they're the ones with the direct relationship to parents/guardians and staff. Vantic processes that data only on the Organization's instruction, under a written agreement with them (see our subscription agreement). If you're a parent, guardian, or player with a question about your own data, your first point of contact is your Organization, not Vantic directly — though we'll always help route the request correctly.

2. Data we collect

Everything below is entered by your Organization's coaching/S&C staff, not collected by Vantic from any other source.

- **Staff account data:** name, email address, role (e.g. Head S&C, Coach), which teams/sports you're assigned to.
- **Organization data:** organization name, club logo, subscription/plan status.
- **Player identity data:** name, date of birth, gender, age group, team/sport, playing position.
- **Performance test results:** numeric results across physical tests (speed, power, strength, endurance, body composition, and sport-specific batteries), including which staff member captured each result and when.
- **Wellness check-in data:** self- or coach-reported daily scores for sleep quality, energy/fatigue, muscle soreness, stress, and mood.

- **Injury and recovery data:** a described injury, the date it occurred, evaluation dates, estimated return-to-training and return-to-play timelines, and rehab guidance/notes entered by staff. A simple readiness flag (green/yellow/red) and short note may also be recorded per player.
- **Usage data:** standard technical data (pages visited, browser/device type) needed to operate and secure the platform.

Vantic does not collect this data directly from players, parents, or guardians — it is entered into the platform by your Organization's own staff, using accounts your Organization controls.

3. How we use it — and what we never do

What we do with your data:

- Provide the platform itself: scoring, benchmarking, dashboards, trend tracking, and program generation for your Organization's own use.
- Communicate with your Organization's staff about their account and support requests.
- Maintain and improve the security and reliability of the platform.
- Facilitate a cross-organization player transfer, but only when your Organization explicitly requests one and it's reviewed and approved — see our Player Transfer & Data Policy for exactly how that works.

What we never do:

- We never use your Organization's data to build products or features for other customers.
- We never train any model — AI, machine-learning, or otherwise — on player or staff data, shared across organizations or otherwise. (Vantic's scoring and program-generation engines are rules-based, not AI/ML.)
- We never use player or staff data for advertising, and we don't run advertising on the platform at all.
- We never share one Organization's individual records with another Organization — each Organization's data (names, individual test results, injury and wellness records) is isolated at the database level, not just in the application. The only two exceptions, described in full in section 5 below, are the anonymized cross-org percentile statistic and an explicitly requested player transfer.

- We never sell or share a player's or staff member's name, surname, email address, password, or an Organization's own name or identity, under any circumstances.

This is a different thing from aggregate, de-identified statistics (e.g. "1 in 10 U13 boys weighs 50kg") — which contain no name, no Organization identity, and no way to trace back to any individual or Organization. Vantic may use and share this kind of aggregate statistic, including for its own marketing or with third parties — see section 5 for exactly how, and the safeguards that apply.

We try to protect all data entrusted to us to the best of our ability — see section 9 for exactly what that means in practice, not just as a promise.

4. Children's personal information and health information — read this section

Most Vantic players are under 18. Under POPIA, personal information about children may generally only be processed with the consent of a parent or legal guardian ("a competent person"), or under another specific legal ground (sections 34–35). Separately, injury, wellness, and similar health-adjacent information is classified as "special personal information" under POPIA and is subject to its own narrow processing conditions (sections 26–27) — a generic privacy policy statement is not, on its own, sufficient justification; each purpose needs a real, documented basis.

How this is handled today: your Organization, as the Responsible Party, is contractually responsible for obtaining appropriate consent from parents/guardians — typically as part of its own enrollment or sports-participation consent process — before entering a player's information into Vantic, and for having a lawful basis for recording health-adjacent data (injury tracking, wellness monitoring) as a normal part of its duty of care to its athletes. Vantic processes this information only for the specific purposes your Organization uses the platform for: performance testing, wellness monitoring, and injury/return-to-play management — not for any other purpose.

To be unambiguous: obtaining, verifying, and keeping proof of parental/guardian consent is entirely your Organization's responsibility, not Vantic's. Vantic does not obtain this consent, does not verify that your Organization has obtained it, and does not store or review any consent record on your Organization's behalf. Vantic's only role is processing the data your Organization has already decided, on its own lawful basis, to enter.

5. Data sharing

We do not sell personal data. We do not share individual player or staff records between Organizations — each Organization's own data (names, individual test results, injury and wellness records) is isolated at the database level and never visible to another Organization.

The one exception is aggregate, anonymized statistics. Vantic computes aggregate numbers — for example, a percentile showing how a team's results compare to others in the same sport, age group, and gender, or a broader statistic like "1 in 10 U13 boys weighs 50kg" — from results pooled across every Organization on the platform. Every such statistic never includes any player's or staff member's name, any Organization's name or identity, or any other identifying detail, and is only computed at all when at least five real results exist in that group, specifically so no individual result can be inferred even indirectly from a small sample.

Vantic uses this kind of aggregate statistic to show your Organization how it compares to others (the in-app percentile feature), and **may also use it for Vantic's own marketing, or share or license it to third parties** (for example, industry or sports-science insights) — always subject to the same protections above: never identifying, never below the five-result threshold, and never traceable back to any individual or Organization.

The other exception is a player transfer your Organization explicitly requests. If your Organization asks to move a specific player's record to a different Organization on Vantic (for example, a player changing schools or clubs), that player's core record moves to the new Organization once the request is reviewed and approved — this is the one case where a player's individual data becomes visible to a different Organization, and it never happens automatically or without your Organization's own request. See our Player Transfer & Data Policy for the full process, including exactly what does and doesn't move.

We share data only with the sub-processors required to run the service, under contract:

- **Supabase** — database, authentication, and file storage hosting.
- **PayFast** — payment processing, once billing is live (not yet active). Only billing-relevant information is shared; player data is never sent to PayFast.

6. Where your data is stored

Vantic's production data is hosted with Supabase in the eu-north-1 (Stockholm, Sweden) AWS region; a separate development/staging environment uses eu-west-1 (Ireland) and never holds real player data. This means personal information is transferred outside South Africa for processing and storage. **The basis for this transfer, under POPIA section 72(1)(a),** is Supabase's own Data Processing Addendum (effective automatically on acceptance of Supabase's terms, published at supabase.com/legal/dpa), which incorporates the EU Standard Contractual Clauses (Commission Implementing Decision (EU) 2021/914). Those Clauses impose data protection obligations substantially similar to POPIA's own conditions on lawful processing, and include restrictions on Supabase transferring data onward to any further country — the two elements POPIA section 72 requires of a qualifying binding agreement. Unlike the GDPR, POPIA does not publish an official list of countries with "adequate" protection; each responsible party assesses and documents its own basis, and this is Vantic's.

7. Data retention

While your Organization's subscription is active, your data is retained for as long as the subscription runs. If a trial ends without a plan being purchased, or a subscription is cancelled, your Organization's access is paused (not deleted) and identifiable data is kept for 90 days — giving you a window to export it or reactivate the subscription.

After that 90-day window, player- and staff-identifying fields (names, dates of birth, email addresses) are permanently deleted. The underlying numeric test and wellness results are kept, but only in de-identified form — no longer linked to a named individual — so your Organization's own historical trend data isn't lost, and so this data can keep contributing, in aggregate only, to the cross-organization percentile benchmark described in section 5. De-identified data of this kind falls outside POPIA's definition of personal information and is not subject to the same retention limits. Your Organization can request full deletion, including of this de-identified data, at any time, rather than waiting for the 90-day window.

8. Your rights

Under POPIA, data subjects (or, for a child, their parent/guardian) have the right to:

- Be notified that personal information is being collected, and why.
- Access the personal information held about them.

- Request correction or deletion of personal information that is inaccurate, irrelevant, excessive, out of date, or unlawfully obtained.
- Object to the processing of personal information in certain circumstances.
- Lodge a complaint with South Africa's Information Regulator if they believe their rights have been infringed.

Requests should go through your Organization first, since they hold the direct relationship with players and parents/guardians — Vantic will support your Organization in fulfilling any valid request. Information Regulator contact details: POPIA complaints — popiacomplaints@inforegulator.co.za; general enquiries — enquiries@inforegulator.org.za; 010 023 5200 (or toll-free 0800 017 160); Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191.

9. Security

Real measures in place, verified 2026-08-12:

- Row-level security is enforced at the database level across every table holding player/organization data (31 tables, 88 policies) — one organization's staff cannot access another organization's data, enforced by the database itself, not just the application.
- All server-side functions that perform privileged actions verify the caller's identity before doing anything.
- Data is encrypted in transit (HTTPS/TLS).
- No passwords or API keys are stored in the application's source code.

Data is encrypted at rest (AES-256), confirmed against Supabase's own published security documentation — this is automatic and requires no separate configuration. Multi-factor authentication is not yet offered to Vantic staff accounts, though the underlying platform (Supabase Auth) supports it — this is a real, currently-open gap, not yet on a committed timeline.

We apply reasonable technical and organizational security measures to protect your data, and treat that as an ongoing responsibility that grows as the platform does, not a box checked once. That said, no online service can guarantee absolute security, and no method of electronic storage or transmission is 100% secure — we can't promise perfection, only genuine, continuing effort to protect what you entrust to us to the best of our ability. If a security compromise affecting your data ever occurs, we will notify your Organization without delay, so your Organization can meet its own

notification obligations to affected individuals and the Information Regulator under POPIA sections 21 and 22.

10. Contact

Questions about this policy: hello@vantic.co.za