

1. Who we are

iRunSA is a digital athletics platform operated as part of the Felonk ecosystem. We support athlete registration, athlete profiles, event participation, official results, verified performances, shareable athlete CVs and federation grade administration. Felonk (Pty) Ltd is the responsible party for personal information processed through iRunSA, unless a separate written agreement states otherwise.

2. Athlete profile and performance information

We process athlete account details, identity or duplicate prevention information, date of birth, gender, province, country, club or school, profile media, biography, event entries, timing data, personal bests, verification evidence, performance history and audit records connected to athlete administration.

Verified athlete CV information may include official iRunSA results, imported official results, manually submitted performances, supporting evidence, verification status, confidence scoring and review history.

3. Guardian and minor athlete information

A minor may not register their own iRunSA account. A parent or guardian creates their own guardian account first, supplying their own name, surname, cellphone number and email address, and then registers each minor athlete in their care from that account.

We process the guardian's name, surname, cellphone number, email address and their relationship to each athlete they register, so that a clear and reviewable line of responsibility exists for every minor athlete profile on the platform.

Guardian information is used only to administer minor athlete accounts, respond to safeguarding concerns and confirm authority over a minor's profile. It is not published and is not used for marketing.

Official event results and performance history may be displayed on a minor athlete's public athletics performance profile. This profile excludes guardian information, date of birth, contact details, addresses, identity documents, medical information, private photos and account controls.

Read our full guide to Minors, Guardians and Athlete Participation.

4. Identity and passport number protection

ID or passport numbers collected for identity verification and duplicate prevention are encrypted at rest in our database. They are never stored or transmitted in plain text.

Encrypted identity numbers can be decrypted only through authorised, authenticated access, for example when an athlete or guardian views or corrects their own profile, or when an authorised administrator performs identity verification or duplicate resolution. Access is logged.

Where an identity number needs to be searched, we use a secure lookup method rather than reading the stored value directly, and only the last four characters are ever shown for reference in an administrative screen.

5. Sharing within the athletics ecosystem

Athlete information, verification data, performance history and profile details may be shared with relevant governing and administrative athletics bodies for athletics related operational, administrative, competitive, development, verification, ranking, compliance and athlete management purposes.

These recipients may include provincial athletics federations, national athletics federations, athlete clubs, coaches, athlete representatives, athlete managers, competition organisers, timing and results service providers, and authorised platform administrators. Examples include Central Gauteng Athletics and Athletics South Africa.

Sharing is limited to athletics related purposes and is intended to support trusted athlete records, event administration, eligibility checks, competition operations, development pathways and federation reporting.

6. Public profiles and field level privacy

Adult athlete, coach, representative, manager and other professional profiles may be publicly discoverable under the applicable profile controls. Minor athlete profiles are private and removed from public search by default, and stay that way unless the registering guardian later enables a specific public profile option.

A public profile may show the person's name, athletics role, club or school affiliation, province, biography, approved profile media, badges and applicable performance information. Identity or passport numbers, authentication data, private verification evidence and full dates of birth are not public profile fields.

Contact details remain controlled separately and are private unless the authorised person explicitly enables the applicable sharing option. Official event results use the event or federation minor results policy and are not controlled only by enhanced public profile consent.

7. Verification, evidence and audit trails

Verification evidence may include result links, PDFs, screenshots, official result data, timing imports, event participation records and review notes. We keep verification audit trails so that athletes, administrators and authorised athletics bodies can understand how a performance was reviewed, matched, accepted, rejected or marked for review.

Verified performances may be used for rankings, selections, qualification, statistical analysis, federation reporting, athlete monitoring and athlete development purposes.

8. Official result integrations and timing providers

iRunSA may receive or process result data from official event systems, timing providers, RFID timing systems, competition organisers and results service providers. This data may be matched to athlete profiles to create official result records, performance history, rankings and verified athlete CV entries.

9. Shareable CV links, QR codes, PDFs and media uploads

Athletes and authorised representatives may create shareable live profile links, QR codes and PDF outputs. Live profile sharing is preferred because it reflects current verification and field level sharing settings. PDF exports are static snapshots and may become outdated after generation.

Media uploaded for use on a profile or CV must be lawful to use and may be displayed publicly. Evidence uploaded only for verification is not treated as public profile media.

10. Governing body, coach and manager access

Authorised federation administrators, coaches, managers and athlete representatives may access athlete information where needed for legitimate athletics administration. Access should be role based, proportionate and connected to the relevant athlete, club, event, province, federation or administrative responsibility.

11. Lawful basis and POPIA principles

We process personal information to perform platform services, administer athlete records, support legitimate athletics ecosystem interests, comply with legal or regulatory duties, protect platform integrity and, where required, based on consent. We apply POPIA principles of purpose specification, processing limitation, openness, security safeguards, data subject participation and accountability.

We do not sell athlete personal information.

12. Retention

Account and profile information is retained while the account or athlete record remains active and for a reasonable period afterwards where required for dispute resolution, legal compliance, fraud prevention or athletics administration. Official results, participation records, verification audit trails and federation reporting records may be retained for longer because they form part of the sanctioned athletics record.

13. Your rights

You may request access, correction, deletion, restriction, objection or withdrawal of consent where applicable under POPIA. Some requests may be limited where official competition records, legal obligations, federation administration or legitimate athletics record keeping require continued retention.

Send privacy requests to support@irunsa.co.za with the subject line "POPIA Rights Request".

14. Security

We use technical and organisational safeguards including encryption of sensitive identity numbers, access controls, TLS, platform logging, role based administration and cloud security controls. No online platform can guarantee absolute security, so users should keep passwords secure and report suspicious activity promptly.