

LEGAL DOCUMENT

Vela Privacy Policy

Version 1.0

Effective date: 4 September 2026

Contents

Version: 1.0 | Effective date: 4 September 2026

1. About this Privacy Policy . . . 3

2. Who this Privacy Policy applies to . . . 3

3. Responsibility for personal information . . . 3

4. Personal information Vela processes . . . 4

5. Where personal information comes from . . . 7

6. Why Vela processes personal information . . . 7

7. Justifications for processing . . . 8

8. Who can access or receive personal information . . . 8

9. Cross-border processing . . . 9

10. Operational statistics, ratings and automated processing . . . 10

11. Retention, availability, deletion and de-identification . . . 10

12. Security safeguards . . . 12

13. Your privacy rights . . . 13

14. Children's personal information . . . 14

15. Privacy contact and Information Officer . . . 14

16. Changes to this Privacy Policy . . . 14

1. About this Privacy Policy

Vela is a property management, maintenance coordination, communication and record-keeping platform for landlords, landlord-business team members and tenants.

Vela is currently being made available to a limited number of users for testing and evaluation (the **Testing Phase**). During this phase, features and workflows may change, and some privacy requests or operational processes may be handled manually. The Testing Phase does not change Vela's obligations under POPIA or other applicable law, or limit any person's privacy rights.

This Privacy Policy explains how personal information is collected, used, stored, shared and protected when someone creates or uses a Vela account, participates in a Vela workspace or workflow, contacts Vela, or otherwise interacts with the platform.

This Privacy Policy is a notice about the processing of personal information. It is not a request for blanket consent and does not replace Vela's General Terms and Conditions or any additional role-specific terms.

Vela processes personal information in accordance with the Protection of Personal Information Act 4 of 2013 (POPIA) and other applicable South African law.

Platform provider and responsible party

- **Platform provider:** Aidan Murray Parsons and Dylan Ezterhuisen, jointly operating under the trading name Vela
- **Trading name:** Vela
- **Legal status:** Two natural persons jointly operating an unincorporated business; Vela is not incorporated and has no registration number
- **Physical address:** Vela is operated remotely by Aidan Murray Parsons and Dylan Ezterhuisen from separate private premises and does not currently maintain a public office.
- **Privacy contact:** support@velaproperties.co.za

Aidan Murray Parsons and Dylan Ezterhuisen currently operate Vela jointly and determine the purposes and means of Vela's processing of personal information. They are therefore identified jointly as the responsible party in this Policy.

2. Who this Privacy Policy applies to

This Privacy Policy applies to:

- tenants who create an account or participate in lease and maintenance workflows;
- people who create or manage a landlord business on Vela;
- employees, administrators, property managers, assistants and other team members invited into a landlord-business workspace;
- people whose information appears in a record uploaded to Vela, such as a lease, maintenance attachment or emergency-contact record;
- people who contact Vela for support, feedback, privacy requests or general enquiries; and
- people whose devices connect to the Vela web application.

Service-provider marketplace functionality and active service-provider registration are not currently available and are not described as live services in this Policy.

3. Responsibility for personal information

Vela is responsible for the personal information it processes for its own account administration, platform operation, security, support, legal compliance and service-improvement purposes.

Landlord businesses and other business users decide why and how much of the tenant, property, lease and maintenance information under their control is added to a Vela workspace. Depending on the circumstances, they may be responsible parties for that information and Vela may process it on their instructions as an operator. Vela remains responsible for its own platform, access controls, records, security practices and handling of personal information.

Responsibility may differ depending on the information concerned and how it is used. You may send any privacy request to Vela. If the request concerns information managed by a landlord business, Vela may need to work with that business to respond. Vela remains responsible for its own legal duties.

4. Personal information Vela processes

The current platform may process the categories described below.

Account and contact information

- First name and surname.
- Email address and optional telephone number.
- Email-and-password credentials processed through Supabase Auth for account creation and sign-in. Passwords are supplied to Supabase Auth rather than stored in Vela's application profile records.
- Authentication account identifier, account status and assigned platform role.
- Account, registration and login-related records.
- Failed-login counters, lockout status and related timestamps associated with a normalised email address where Vela's login security controls are triggered.

Workspace, invitation and permission information

- Business and tenant invitation codes and their status.
- The person who created or used an invitation and the relevant date and context.
- Business membership, role and permission records.
- Records of permission changes, workspace access and selected administrative actions.

Landlord-business information

Where a person creates or manages a landlord-business profile, Vela may process:

- legal and trading names;
- entity type;
- business email address, telephone number and primary location;
- website address, tagline and biography; and
- authority confirmations and onboarding acknowledgements.

Property, unit, tenant and lease information

- Property names, descriptions and structured addresses.
- Unit numbers, physical characteristics, facilities, occupancy status and related management information.
- Property information supplied for authorised occupants and business users, including emergency guidance, important contacts, access and security information, utility or service details, property routines, schedules and other useful property instructions.
- Tenant-to-unit and tenant-to-lease relationships.
- Records of ending a tenant's active platform link to a unit, including the selected reason, time and authorised business user responsible for the action. Ending this platform link does not by itself terminate or change the legal lease.
- Lease dates, status, notice period and recorded rent or deposit amounts.

- Tenant emergency-contact name and telephone number where a tenant chooses to add them.
- Lease documents and other information contained in documents uploaded by authorised users.

Vela processes limited monetary terms supplied as part of property, unit and lease records, including stated rent and deposit amounts and rent-escalation information. These are contractual and property-management records, not payment transactions. Vela does not currently collect rent, receive or hold deposits or other funds, process payments, record whether an amount has been paid, maintain a transaction ledger, issue invoices or receipts, calculate tax, or provide accounting or tax-reporting services.

Electronic lease-signing information

Where the electronic-signing workflow is used, Vela may process:

- signature and initial images supplied by signers and witnesses;
- signature-field positions;
- signer names and email addresses;
- the signer's IP address and the date and time of signing;
- the signing method and signing deadline;
- document hashes and audit-certificate information; and
- the resulting signed PDF.

Maintenance information

- Property, unit and room or location context.
- Issue category, specific issue, description, priority and emergency indicator selected by a user.
- Ticket status, changes, rejection or cancellation reasons and event history.
- Messages, sender details, read markers and timestamps.
- JPEG, PNG or WebP photographs and MP4 videos uploaded to a ticket.
- File name, file size, file type, upload details and later removal status.

Users should avoid including unnecessary identity, financial, health or other sensitive information in maintenance descriptions, messages and attachments.

Ratings information

- Rating prompts linked to a resolved maintenance ticket.
- Structured answers and scores supplied by a tenant or an authorised business user.
- Rater and rated-party identifiers and display names.
- The date and context of a rating.
- Aggregate average scores and rating counts.

The current ratings workflow does not accept free-text rating comments.

A user may contact Vela to question the accuracy or handling of personal information in a rating record. Vela will assess the request under applicable law and, where appropriate, consult the relevant landlord business or other participant. This does not limit any statutory right to request correction, deletion or restriction of personal information.

Reports, audit and acceptance records

- Information used to generate portfolio, rent-roll, lease-expiry and maintenance reports for authorised business users.
- Export requests and report filters where recorded by the platform or its infrastructure.
- Audit records identifying the actor, action, target, workspace context and timestamp for selected events.

- The version and date of Terms acceptance and other onboarding acknowledgements.
- Published legal-document versions and current PDF files made available for viewing or download.

Vela may use recorded property and lease terms to calculate management summaries such as expected monthly rent, recorded deposit totals, average contractual rent and projected rent after an escalation. These figures do not establish that an amount has been invoiced, paid, received, remains outstanding or is actually held. Report files currently generated for download are not maintained by Vela as a separate accounting or tax-report archive.

Notifications and delivery information

Where Vela creates an in-platform notification or attempts to send a transactional email, it may process:

- the recipient's profile and email address;
- the notification category and its connection to a business, property, unit, maintenance ticket or other relevant record;
- created, read, digested or resolved status and timestamps where applicable; and
- limited delivery records, including the provider message identifier, delivery result, attempt count and failure reason.

Notification records do not store a separate full copy of every underlying record. A notification may nevertheless display limited names, references, statuses, prompts or message excerpts needed to explain the event. Dismissing a notification or clearing read notifications deletes the applicable notification rows, but does not delete the underlying platform record to which a notification relates.

Technical, authentication and security information

Depending on the activity and the infrastructure involved, Vela and its service providers may process:

- IP addresses captured as part of lease-signing evidence and IP information generated by an infrastructure provider where applicable;
- authentication and session identifiers and related records used to sign users in, maintain sessions and protect account access;
- account, request and activity timestamps, including message read markers and recorded audit events;
- limited browser or user-agent information where it is generated by an infrastructure provider or collected for a stated security or evidential purpose;
- application, notification and email-delivery errors where those events are recorded by Vela's application or providers;
- limited hosting, database, storage and authentication-service logs generated by the applicable provider; and
- information required to investigate abuse, attempted unauthorised access or a security incident.

Failed-login records are restricted to server-side security processes and are not available to ordinary platform users. A successful login resets the applicable failed-attempt state. These controls are intended to slow repeated attempts and do not prove that the person associated with an email address made a particular attempt.

Vela does not currently maintain a custom log of every ordinary page view or request and does not currently use a third-party behavioural- or product-analytics service. Vela's hosting and other infrastructure providers may nevertheless generate limited technical logs in the normal operation, security and troubleshooting of the platform. In this Policy, routine technical logs does not mean a user's lease, maintenance history, business audit trail or lease-signing evidence, which are covered separately. Before enabling an optional analytics service, Vela will assess the information it would collect, its purpose, retention, provider access and any cookie or consent requirements, and will

update this Policy and any user notice where required. The precise production-provider logs and settings must be confirmed before this Policy becomes effective.

Feedback, support, misuse reports and enquiries

When a user submits a support request, bug report, feature request, general feedback, privacy request or misuse report, Vela may process the submitter's profile, name and role; the selected type, category, affected area, urgency and impact; the title and information entered in the form; the page from which the user entered the Feedback area and the specific feedback-form page used to make the submission; limited device information supplied with a bug report; supported screenshot attachments; status and resolution information; and related internal review or audit records.

These submissions may contain information about another person, business, property, lease or maintenance matter. Users should provide only information reasonably necessary for Vela to understand and respond to the submission. Feedback attachments are stored in private storage and are made available only through restricted platform processes.

5. Where personal information comes from

Vela obtains information from the following sources. Some of this information is personal information because it identifies a person or can reasonably be linked to one.

- **directly from the person concerned**, such as during registration, profile editing, lease signing, maintenance reporting, ratings or support contact;
- **from an authorised landlord or business user**, such as when that user creates a workspace record, uploads a lease, sends an invitation or adds information concerning a property, unit, tenant or maintenance issue;
- **from other platform participants**, such as through messages, ratings, status changes or documents concerning an interaction;
- **automatically from use of the platform**, such as timestamps linked to an account or activity, audit events, authentication records, IP addresses and technical logs; and
- **from Vela's infrastructure and communication providers**, where they return delivery, security, authentication or operational information to Vela.

If you provide information about another person, please provide only what is reasonably necessary and make sure that you have a proper reason to share it. Where appropriate, you should tell the person that their information has been provided to Vela and direct them to this Privacy Policy.

6. Why Vela processes personal information

Vela may process personal information to:

- register, authenticate and administer accounts;
- create and administer landlord-business workspaces;
- apply roles, permissions and access restrictions;
- link tenants to their relevant units and leases;
- store, display and provide authorised access to lease documents;
- facilitate and record electronic lease-signing actions;
- receive, coordinate and preserve maintenance tickets, attachments and communications;
- provide service-related notices, prompts and communications within Vela or by transactional email;
- produce reports for authorised business users;
- operate the structured ratings workflow and calculate rating aggregates;
- maintain audit, acceptance and security records;

- provide support and respond to requests or complaints;
- detect, prevent and investigate security incidents, fraud, misuse or unlawful activity;
- establish, exercise or defend legal rights and comply with legal obligations; and
- understand platform performance and improve current functionality using appropriately limited, aggregated or de-identified operational information where reasonably possible.

Vela does not currently use personal information for targeted advertising, sell personal information, or make automated legal-compliance, housing-eligibility, eviction or lease-validity decisions.

7. Justifications for processing

Vela does not rely on one justification for every processing activity. For the current platform, personal information may be processed where this is necessary to:

- take steps requested by a user or provide the Vela platform under Vela's General Terms;
- comply with an obligation imposed by law;
- protect a legitimate interest of the person concerned; or
- pursue a legitimate interest of Vela, a landlord business or another platform participant, after considering the person's rights and reasonable expectations.

Vela needs to process certain personal information to create and secure accounts, apply access controls, connect users to the appropriate workspace and provide the platform features they choose to use. If this information is not provided or cannot be processed, Vela may be unable to create or maintain the account or provide the relevant feature. Where information is optional, Vela will identify it as such where it is collected.

Accepting the General Terms creates the agreement under which Vela provides the platform. Acknowledging this Privacy Policy confirms that the user has received information about Vela's processing practices. Neither gives Vela unrestricted permission to process personal information. Vela must have an applicable lawful justification for each processing activity.

8. Who can access or receive personal information

Within a landlord-business workspace

- A tenant can access the lease, unit, maintenance and related records made available in their own tenant context.
- Landlord-business owners and team members can access workspace information according to their membership and assigned permissions.
- A maintenance ticket, including its messages and attachments, is available to the tenant associated with that ticket and to members of the relevant landlord business who have permission to view maintenance information.
- Signed lease documents and signing records are available only to the tenant linked to the lease and to authorised Business users with permission to access that lease.
- Business owners can access the business audit log.
- In the current platform phase, a tenant can view only the average score and rating count associated with ratings that tenant has received. Authorised business users with the relevant permission can view only the average score and rating count received by their own business.
- When an authorised business user with permission to assign a lease enters an existing tenant's email address during an invitation, Vela may show only the tenant's aggregate maintenance-reporting helpfulness score and rating count. Individual rating responses are not shown. This aggregate concerns the tenant's helpfulness when reporting maintenance issues. It is not a general tenant rating and does not prove the tenant's suitability, creditworthiness or conduct.

Authorised users may download reports, lease documents and other records. Once a user has lawfully downloaded a copy, that copy is held outside Vela's platform controls and must be handled lawfully by the person or business that downloaded it.

Infrastructure and communication providers

Vela uses the following providers for current platform functions:

- **Supabase** provides authentication, database services and private file storage. Supabase receives and stores the account, workspace, lease, maintenance, feedback and other platform information described in this Policy as necessary to provide those services. Vela's production Supabase project uses the Central EU (Frankfurt) region.
- **Vercel** hosts and delivers the web application and runs application functions and scheduled processes. Vela uses Vercel's Frankfurt (fra1) compute region. Requests may pass through Vercel's global delivery network. The configured compute region does not by itself restrict every request, log or other item of service data to that region.
- **Resend** delivers transactional email communications. Depending on the notification, Resend may receive the recipient's email address and limited service-related content necessary to deliver and explain the message. This may include a name, role, reference to a platform record, limited message content or action prompt. Vela uses Resend's Ireland (eu-west-1) sending region. This determines where an email is dispatched, but Resend states that account data, email metadata, logs and API records are stored in the United States.
- **Google Fonts** delivers fonts and interface symbols to a user's browser. The browser connects directly to Google's servers, which necessarily receive technical connection information such as the user's IP address and browser headers.

Where a provider processes personal information for Vela as an operator, Vela must ensure that an applicable written agreement requires appropriate security measures and addresses matters relevant to the service, such as confidentiality, authorised processing, security incidents, subprocessors and deletion or return of information. This may be contained in the provider's applicable terms and data-processing addendum rather than in a separately negotiated agreement.

Other disclosures

Vela may disclose information where reasonably necessary:

- to comply with applicable law or a lawful court, regulator or law-enforcement requirement;
- to investigate or respond to suspected fraud, misuse, security incidents or threats to safety;
- to obtain professional legal, compliance, accounting or security assistance subject to appropriate confidentiality duties; or
- to establish, exercise or defend legal rights.

Vela does not sell personal information.

9. Cross-border processing

The infrastructure and communication providers identified in section 8 may process or store personal information outside South Africa. Their current configured regions and relevant location qualifications are stated with each provider in that section.

Where personal information is transferred to a recipient in another country, Vela will use a basis permitted by section 72 of POPIA. Depending on the circumstances, this may include an applicable foreign law, binding corporate rules, a binding agreement that provides an adequate level of protection, consent, or another ground permitted by law.

10. Operational statistics, ratings and automated processing

Vela calculates operational information from platform records, including maintenance resolution times, portfolio totals, lease-expiry information and rating averages. Authorised reports may contain identifiable information where necessary for the business user requesting the report.

Where Vela uses information to understand general platform performance or feature use, it will limit the information to what is necessary and use aggregated or de-identified information where reasonably possible. Vela does not currently use a third-party behavioural-advertising or product-analytics service.

Vela does not currently make decisions that have legal consequences or similarly significant effects on a person solely through automated processing. Ratings, reports, reminders and platform statuses are administrative records and aids; they are not automated legal or compliance determinations.

11. Retention, availability, deletion and de-identification

Vela keeps personal information only for as long as it is authorised and reasonably needed for the purpose for which it was collected or subsequently processed. The normal Testing Phase periods below are intended to give users clear expectations. They may be shortened where Vela is no longer authorised to retain a particular record, or extended where retention is required by law or reasonably necessary for an existing or reasonably anticipated dispute, legal process, regulatory matter, security investigation or other lawful purpose.

Record category	Normal retention period	Ordinary in-platform availability
Account and profile information	While the account is active and for up to 90 days after account closure takes effect, except for limited information that forms part of another lawfully retained record.	Available to the account holder while the account remains open. After closure, information that is still retained may be requested under section 13 within 90 days.
Landlord-business, property, unit and workspace records containing personal information	While the workspace is active and for five years after it closes, subject to any shorter period applicable to a particular person's information.	Available to authorised business users while the workspace remains open and their permissions continue.
Workspace membership, permissions and invitation records	Current membership and permission information is kept while the relationship continues. Used invitation and permission-history records are kept for five years after the relevant workspace relationship ends. Unused or expired invitations are kept for up to 30 days after expiry.	Current information is available according to workspace permissions. Historical records are available only where the platform provides an authorised history view or through an applicable request process.
Lease, tenancy and signing records, including recorded rent and deposit terms, lease PDFs, signatures, signing timestamps, signer details, IP evidence and document hashes	Five years after the relevant tenancy ends.	The tenant and appropriately authorised business users may continue to view the historical lease and available document during that period while their accounts or workspace access remain open. Historical access is read-only.

Record category	Normal retention period	Ordinary in-platform availability
Maintenance ticket descriptions, messages, event histories and status information	Five years after the later of the ticket being closed or the relevant tenancy ending.	The tenant linked to the ticket, where there is one, and appropriately authorised business users may continue to view the historical ticket during that period while their accounts or workspace access remain open. This covers tickets submitted by either a tenant or an authorised business user, including tickets concerning a vacant unit that have no linked tenant.
Maintenance photographs, videos and other attachment files	90 days after the ticket is closed. For this purpose, closed means resolved, cancelled or rejected. The underlying ticket record may be retained for the longer period stated above. Limited file metadata and a record that an attachment was removed may remain with the ticket.	Available to the people authorised to view the ticket until the attachment-retention period ends, unless earlier removal is lawfully requested or required.
Report views and generated report files	Vela does not ordinarily retain generated report files as a separate archive. The information used to generate a report is retained according to the applicable source-record category in this table.	Report views remain available to authorised Business users while the relevant Workspace, source records and reporting functionality remain available. A downloaded report is held outside Vela's platform controls.
Ratings and rating prompts	Submitted ratings and their fulfilled prompts are retained while they form part of the active rating history of the rated account or business. They may be retained for up to five years after that account or business closes where reasonably required for complaints, disputes or record integrity. Current Testing Phase averages and counts are calculated from all submitted ratings still retained and do not use a rolling time window.	Available only to the audience described in this Policy and permitted by the applicable platform controls.
Terms acceptance records	Five years after the relevant account or contractual relationship ends.	The account holder can access accepted legal documents through the legal section of their Profile while their account and that functionality remain available. Information that is retained after ordinary access ends remains subject to applicable access rights.
Business audit records	Two years after the recorded event. An audit record may be retained for the longer period applicable to an associated security incident, complaint or dispute, or where longer retention is otherwise reasonably necessary for a lawful purpose.	A Business Owner can access the Business audit log while the Workspace remains open and their owner access continues. Retention after that access ends does not require Vela to keep the Workspace or audit-log interface available.

Record category	Normal retention period	Ordinary in-platform availability
Feedback, support requests, bug reports, feature requests, privacy requests, general feedback and misuse reports, including attachments	Up to two years after the submission is closed or the last substantive contact, unless it becomes relevant to another retained record, complaint, dispute, security matter or legal process.	The submitter may view supported submission types while that feature and their account remain available. Internal access is restricted to authorised Vela personnel.
Routine authentication, in-platform notification, notification-delivery and application-error records	Up to 90 days after creation. A record relating to a confirmed security incident may be kept while the incident is investigated and for up to five years after the investigation closes where reasonably needed for security, proof or legal compliance.	Some current in-platform notifications are visible to their recipient. Other technical and delivery records are not ordinarily displayed, but personal information still held remains subject to applicable access rights.

Retention is different from ordinary in-platform availability. Ending a tenancy, closing an account or losing access to a workspace does not necessarily require immediate deletion of every related record. Conversely, retaining a record does not require Vela to keep an account or workspace active. If direct access has ended, a person may request access to personal information that Vela still holds as explained in section 13, subject to applicable legal limits and the rights of other people.

Vela may pause scheduled deletion where a record is relevant to an existing or reasonably anticipated dispute, legal process, regulatory matter, security investigation or valid access request. Use of information preserved for one of these purposes will be restricted appropriately. Once the reason for the hold ends, the ordinary schedule will resume unless another lawful basis applies.

Vela does not currently maintain a separate backup of platform records or uploaded files. If Vela enables a backup process in future, it will first establish appropriate access, security, retention and deletion controls and update this Policy where required.

Vela cannot delete copies previously downloaded by authorised users. When Vela is no longer authorised to retain personal information, it will delete or destroy the record so that it cannot be reconstructed in an intelligible form, or de-identify it as soon as reasonably practicable and as required by law.

12. Security safeguards

Vela uses technical and organisational measures intended to protect the integrity and confidentiality of personal information and to reduce reasonably foreseeable risks of loss, damage, unauthorised destruction, unlawful access or unlawful processing.

The current codebase includes safeguards such as the following, subject to the verification work noted below:

- authenticated user accounts and session controls;
- role and permission controls in the user interface and selected server-side functions;
- database row-level security for configured tables and server-side authorisation checks in selected routes;
- private storage for lease documents and maintenance attachments;
- time-limited signed links for authorised document and media access;
- inactivity logout controls;
- audit and event records for selected sensitive actions; and
- restrictions on the information made available to each platform role.

No internet-based service can guarantee absolute security. Vela remains responsible for taking appropriate and reasonable measures for its own platform and for reviewing and improving those measures as risks and functionality change.

If there are reasonable grounds to believe that an unauthorised person has accessed or acquired personal information, Vela will investigate, contain and respond to the compromise and notify the Information Regulator and affected data subjects where and as required by section 22 of POPIA.

13. Your privacy rights

Subject to POPIA, PAIA and other applicable legal limits, a data subject may:

- ask whether Vela holds personal information about them;
- request access to a record or description of that information;
- request correction or deletion of inaccurate, irrelevant, excessive, out-of-date, incomplete, misleading or unlawfully obtained information;
- request destruction or deletion of information that Vela is no longer authorised to retain;
- object, on reasonable grounds relating to their particular situation, to processing based on specified legitimate-interest grounds;
- withdraw consent where a particular activity relies on consent;
- ask Vela to restrict use of a contested record where required by law; and
- lodge a complaint with the Information Regulator or pursue another remedy available under law.

Confirmation of whether Vela holds personal information is free. Access to copies or records may be subject to a prescribed or legally permitted fee. If a fee is permitted, the requester will be informed before the request is completed.

During the current platform phase, privacy requests may be submitted by email to support@velaproperties.co.za. This includes requests to access, correct or delete personal information, objections to processing and other privacy enquiries. Vela may ask for information reasonably necessary to verify the requester's identity or authority and to protect information from unauthorised disclosure. Vela will handle each request under the procedure and within the period required by POPIA, PAIA or other applicable law.

Detailed procedures for requesting access to records will be provided in Vela's separate PAIA manual. Correction, deletion and objection requests will be handled under the applicable POPIA process. This Privacy Policy summarises these rights but does not replace the PAIA manual or a prescribed request form where one applies.

Where a request concerns information controlled by a landlord business, Vela may need to coordinate the request with that business. Vela will not use that allocation of responsibility to avoid its own duties.

PAIA access requests

A Privacy Policy does not replace a PAIA manual. Before the Testing Phase begins, Vela must prepare and make available its PAIA manual and prescribed access-request process:

- **PAIA manual:** Free by email request from support@velaproperties.co.za and, once published, through Vela's website
- **PAIA request contact:** support@velaproperties.co.za

Complaints to the Information Regulator

A person may contact the Information Regulator (South Africa) using the details published on its official website:

- **Website:** https://inforegulator.org.za/
- **Email:** enquiries@inforegulator.org.za

- **Telephone:** 010 023 5200

14. Children's personal information

Vela accounts are intended for people aged 18 or older. A person under 18 should not create or operate their own Vela account during the current platform phase because Vela has not implemented an age-verification or competent-person consent workflow.

A lease, household record, maintenance attachment or other user-supplied document may nevertheless contain information about a child. Users should not add children's personal information unless it is necessary, lawful and appropriately authorised. Vela will restrict or remove children's information where required by law and will seek any prior authorisation required from the Information Regulator before undertaking processing that requires it.

Anyone who believes that a child has created an account or that children's information has been processed inappropriately should contact Vela using the details below.

15. Privacy contact and Information Officer

Questions, privacy requests and concerns may be sent to:

- **Responsible party:** Aidan Murray Parsons and Dylan Ezterhuisen, jointly operating under the trading name Vela
- **Information Officer:** Dylan Ezterhuisen
- **Email:** support@velaproperties.co.za
- **Physical address:** Vela is operated remotely by Aidan Murray Parsons and Dylan Ezterhuisen from separate private premises and does not currently maintain a public office.

Dylan Ezterhuisen is the intended Information Officer.

16. Changes to this Privacy Policy

Vela may update this Privacy Policy when its practices, platform functionality, service providers or legal obligations change.

The current version and effective date will be made available with the Policy. Where a change is material, Vela will provide reasonable notice through an appropriate channel, such as an in-platform notice or email. Vela will request fresh consent or acknowledgement where the nature of the change or applicable law requires it.

Continued use of Vela will not be treated as consent to a new processing activity where valid consent is legally required.