Privacy & POPIA Policy

Castor Project Consultants (Pty) Ltd

Registration number: 2021/161461/07
Effective date: 3 October 2026
Version: 1.0

1. Introduction and scope

Castor Project Consultants (Pty) Ltd ("CPC", "we", "us" or "our") respects privacy and is committed to processing personal information lawfully, reasonably and securely. This Privacy & POPIA Policy explains what personal information we collect, where it comes from, why we process it, how we use and share it, how long we retain it, the safeguards we apply, and the rights available to data subjects.

This policy applies to CPC's public website at castorprojects.com, the secure CPC NPO application at npoapp.castorprojects.com, CPC online forms and communications, the CPC NPO Compliance Platform, and other CPC consulting, software, project, government, municipal, NPO and professional-service activities where CPC determines the purpose and means of processing personal information.

Where CPC processes personal information strictly on behalf of a client under that client's instructions, CPC may act as an operator rather than the responsible party. In those cases, the client's privacy notice and the applicable operator/data-processing agreement may also apply.

This policy should be read together with CPC's Terms of Use / Terms of Sale, applicable product or service terms, document licence / permitted-use terms, Refund & Fix Guarantee and any project-specific notices.

2. Responsible party and Information Officer

For processing activities where CPC determines the purpose and means of processing, the responsible party is:

- Entity: Castor Project Consultants (Pty) Ltd
- Registration number: 2021/161461/07
- Physical / registered address: 27 Outeniqua Street, Noordheuwel, Krugersdorp, 1739, South Africa
- General privacy/contact email: info@castorprojects.com
- Telephone: +27 81 645 9338

CPC's Information Officer / privacy contact is responsible for overseeing POPIA and PAIA compliance, handling data-subject requests, coordinating security-compromise response and maintaining appropriate privacy governance.

- Information Officer: Stephan Haupt
- Email: stephan@castorprojects.com or info@castorprojects.com

3. Personal information we may collect

The categories of personal information CPC processes depend on the website, platform, service or project being used. We apply data minimisation and seek to collect only information reasonably necessary for the relevant purpose.

Public website, contact and enquiry information may include:

- name and surname, organisation or NPO name, job title or role, email address, telephone/mobile number and location;
- enquiry type, service area, message, project information and any attachment voluntarily submitted;
- communication preferences and records of consent, objection, unsubscribe or suppression.

Account and secure-platform information may include:

- email address, mobile number, authentication and account status information, NPO membership/role and permission information;
- NPO name, registration number, organisation type, sector, province, municipality/area, financial year-end, contact details and permanent CPC Reference;
- Primary Administrator and Authorised User information, authority-verification information and audit records;
- account, password-reset, PIN-reset, session, security-event and access-control metadata. CPC does not store plaintext passwords.

Commercial and service information may include:

- products/Tiers selected, orders, invoices, payment status, Manual EFT proof, payment references, refunds/cancellations, entitlements and download events;
- CPC Assistance requests, quotations, work status, client-visible comments, internal operational notes and service-delivery records;
- document licences, issued-document references, document versions and release/re-release history.

Uploaded documents and compliance records may include registration certificates, constitutions, governance records, financial statements, management accounts, annual reports, DSD correspondence, identity/leadership evidence and other supporting documents relevant to a legitimate CPC/NPO workflow.

Technical and usage information may include IP address, device/browser information, session and security logs, page or feature usage, source/referrer information, cookie or similar identifiers where used, and audit/event data needed for security, troubleshooting, legal compliance and service improvement.

4. Sources of personal information

CPC generally obtains personal information directly from the data subject or an authorised representative. We may also obtain information from:

- an NPO, company, government body, municipality, client or authorised representative with whom the person is associated;
- publicly accessible or official sources, including public registers, government/NPO information sources, organisation websites or legitimate business directories, where collection and further use are lawful;
- existing CPC business records, service interactions, project records and prior lawful communications;
- approved service providers or operators, for example payment, email-delivery, security, hosting or verification providers;
- bulk-import source files supplied or lawfully obtained by CPC, subject to staging, validation, approval and privacy controls.

Where POPIA requires CPC to provide notice of indirect collection, CPC will do so unless a lawful exception applies.

5. Special personal information and information about children

The CPC NPO Platform is intended primarily for authorised adult representatives of organisations. CPC does not seek to collect special personal information or children's personal information merely because an NPO works in a sensitive sector.

Some legitimate NPO, compliance, consulting or project workflows may nevertheless involve information that POPIA treats as special personal information or information about children. CPC will process such information only where it is necessary, relevant and lawfully authorised, and will apply additional access, confidentiality and security controls where appropriate.

Users should not upload unnecessary identity documents, health information, banking credentials, children's information, criminal information, religious or political information, or other sensitive material unless the relevant CPC workflow specifically requires it and the user is authorised to provide it. CPC may reject, quarantine, restrict or request removal of unnecessary sensitive information.

6. Why we process personal information

CPC processes personal information on one or more grounds permitted by POPIA, including consent where required, performance of or steps toward a contract, compliance with legal obligations, protection of a legitimate interest of the data subject, and pursuit of CPC's or a third party's legitimate interests where lawful and proportionate.

Purposes include:

- responding to enquiries and providing information about CPC services;
- creating and administering user accounts and NPO profiles;
- verifying email addresses, authority, permissions and protected profile changes;
- maintaining the one-NPO / one-CPC-Reference / one-Master-Profile model;
- processing product/Tier selections, orders, invoices, payments, refunds and cancellations;
- releasing purchased documents and enforcing entitlement, download, re-release and document-licence controls;
- providing CPC Assistance, professional services and paid Assisted Completion where agreed;
- calculating and administering approved compliance dates, reminders and service notifications;
- receiving, classifying, quarantining, malware-scanning, validating and securely storing permitted uploads;
- maintaining audit trails, security controls, fraud prevention, incident response, backups and recovery processes;
- operating, maintaining, troubleshooting and improving CPC websites, systems and services;
- carrying out lawful marketing and customer communications subject to consent, objection, unsubscribe and suppression rules;
- meeting legal, regulatory, accounting, tax, contractual, dispute-resolution and record-keeping obligations;
- establishing, exercising or defending legal rights and protecting CPC, its clients, users and systems.

7. CPC NPO Platform - role and limitations

The CPC NPO Platform supports NPO administration, document products, compliance reminders and CPC services. CPC is not the Department of Social Development (DSD) and does not represent that CPC Reviewed status means DSD verification, legal compliance or DSD approval.

CPC does not submit an NPO's application or compliance return to DSD on the NPO's behalf unless a separate, expressly agreed professional engagement states otherwise. The NPO remains responsible for reviewing its information and making any

required submission to the appropriate authority. CPC does not guarantee that DSD or another authority will approve or accept any submission.

Phase 1A is not a general-purpose cloud drive. Upload functionality is restricted to legitimate CPC/NPO workflows and supporting evidence.

8. Orders, payments and financial information

CPC may process payment-related information needed to create orders, issue invoices, reconcile payments, release products, manage refunds and maintain financial/audit records.

Online card payments are processed by an approved third-party payment gateway. CPC does not intentionally collect or store full card numbers, CVV/CVC values or other raw card credentials. The payment provider processes those details under its own legal and security obligations and returns transaction/status information needed by CPC.

Manual EFT remains an available payment method where offered. CPC may process bank/payment references and proof-of-payment documents for reconciliation. Proof of payment alone does not constitute server-side confirmation of an online card payment.

9. Uploads, document handling and malware scanning

Permitted customer and CPC uploads are placed into a segregated quarantine process before they are treated as trusted files. Files are validated for applicable file type, size, workflow context and security status.

For Phase 1A, CPC uses a managed malware-scanning service to scan permitted uploads. Files that cannot be confirmed as clean are rejected, isolated or placed into security review and are not made available as trusted NPO documents.

The Phase 1A platform upload limit is 3.5 MB per file. Where a legitimate document exceeds the platform limit, the user should first compress or rescan it. If this is not practical, the user may contact CPC for a controlled manual alternative. An oversized file sent outside the platform is not automatically treated as trusted platform content and must be handled under CPC's manual security process before use or import.

CPC may change the scanner or upload limit in future where usage, security, cost or storage requirements justify it, subject to appropriate provider/privacy review and platform change control.

10. Communications, notifications and direct marketing

CPC distinguishes between essential service communications and marketing communications.

Security/account and transactional/service communications include email verification, password/PIN recovery, order and payment notices, document release, CPC Assistance updates and approved compliance reminders. These communications are necessary to operate the account or deliver the requested service and are not disabled merely because a person unsubscribes from marketing.

Marketing/CPC communications may include newsletters, promotions, toolkit offers and general CPC updates. Electronic direct marketing is sent only where permitted by POPIA. Where consent is required for unsolicited electronic direct marketing, CPC will obtain and retain evidence of consent using a process that meets the applicable POPIA requirements. Where the existing-customer exception is relied upon, CPC will limit marketing to its own similar products/services and provide an opportunity to object.

Every applicable marketing email will include a practical unsubscribe route. Unsubscribed, suppressed, invalid, hard-bounced or complaint addresses are excluded from future marketing sends as applicable. A recipient who has unsubscribed will not be re-subscribed merely by CPC administrative action; where re-subscription is supported, confirmation by the affected email address is required.

CPC may retain a suppression record after an unsubscribe so that the preference can continue to be respected.

11. Automated processing and recommendations

Phase 1A does not use solely automated decision-making to make decisions that produce legal or similarly significant effects on a person. The platform may automate administrative calculations, reminders, validation, security checks, filtering and workflow routing.

CPC does not automatically determine which commercial Tier an NPO should buy in Phase 1A. Users who are uncertain are directed to CPC support. If CPC later introduces materially significant automated decision-making or AI-assisted profiling, this policy and the applicable user notices will be reviewed before production use.

12. Who we share personal information with

CPC does not sell personal information. We disclose personal information only where reasonably necessary for the purposes described in this policy, where the data subject directs or authorises it, or where disclosure is required or permitted by law.

Recipients may include:

- authorised CPC directors, staff, consultants or contractors who require access for their role;

- technology operators and service providers used for database, authentication, private storage, hosting, DNS/perimeter security, email delivery, malware scanning, payment processing, support, backup or other approved platform functions;
- professional advisers, auditors, insurers or legal advisers where reasonably necessary;
- banks, payment processors and financial-service providers in connection with payments and refunds;
- government bodies, regulators, courts, law-enforcement bodies or other parties where disclosure is lawfully required or justified;
- a purchaser, successor or restructuring party if CPC undergoes a lawful corporate transaction, subject to appropriate confidentiality and privacy safeguards.

Key technology providers used or approved for the CPC NPO Platform may include Supabase (database, authentication and storage), Cloudflare (DNS/perimeter security), Resend (email delivery), Cloudmersive (malware scanning) and an approved payment gateway. This list may change as providers are reviewed or replaced. CPC maintains a controlled Systems & Cost Register and assesses material providers for security, privacy, data-location, cost and dependency risk.

Where a service provider acts as an operator for CPC, CPC seeks to ensure appropriate contractual and security obligations consistent with POPIA, including confidentiality, security safeguards and notification of security compromises.

13. Cross-border processing

Some approved service providers may store or process personal information outside South Africa. Before or while using such providers, CPC considers the nature of the information, the purpose of processing, contractual safeguards, provider security and the requirements of section 72 of POPIA.

CPC will use cross-border processing only where a lawful basis for the transfer exists, including where the recipient is subject to a law, binding corporate rules or binding agreement that provides an adequate level of protection, where the data subject consents where appropriate, or where another section 72 ground applies.

Where practical, CPC will minimise the personal information transferred to an external provider and avoid sending unnecessary sensitive information.

14. How we protect personal information

CPC applies reasonable technical and organisational safeguards appropriate to the nature of the personal information and the foreseeable risks. Controls may include:

- HTTPS/TLS for data in transit and secure provider-managed encryption where applicable;
- private storage and strict NPO-level access segregation;
- role-based permissions, least privilege and server-side authorisation checks;
- mandatory email verification, secure credential storage, password/PIN recovery controls and session/security-event management;
- row-level security and cross-NPO access controls in the application database;
- quarantine and malware scanning of permitted uploads before trusted use;
- server-side protection of API keys, payment/provider secrets and privileged operations;
- audit logging of material security, access, payment, document, admin and change events;
- separate Development/Test and Production environments, with no ordinary use of real client data in Development/Test;
- controlled backups/exports, recovery procedures, change control and rollback processes;
- provider, dependency and security review appropriate to CPC's size, risk and project phase.

No internet transmission, storage system or security control can provide an absolute guarantee of security. CPC therefore maintains layered controls and reviews safeguards as risks, usage and technology change.

15. Security compromises

If CPC has reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, CPC will follow its incident-response process and the notification obligations applicable under POPIA.

Where required, CPC will notify the Information Regulator and affected data subjects as soon as reasonably possible after discovery, taking account of legitimate law-enforcement needs and the information required by POPIA. An operator that experiences a security compromise affecting CPC-controlled personal information is required to notify CPC so that CPC can discharge its responsibilities as responsible party.

CPC records and investigates material security incidents, takes reasonable containment/remediation steps, and reviews controls after the incident.

16. Cookies, analytics and similar technologies

CPC websites and applications may use essential cookies or similar technologies for authentication, session management, security, preferences and core functionality. Where non-essential analytics or similar technologies are used and consent is legally required, CPC will provide an appropriate notice and consent/control mechanism.

Phase 1A analytics are intended to remain proportionate and privacy-conscious, for example measuring page visits, NPO Solutions engagement, registration/login clicks, Tier/pricing engagement and contact/support actions. CPC does not intend Phase 1A analytics to create intrusive behavioural profiles.

Users may control cookies through browser settings, although disabling essential cookies or storage may prevent some secure-platform features from operating correctly.

17. Retention, deletion, archiving and de-identification

CPC retains personal information only for as long as there is a lawful and reasonable need for the relevant purpose, including service delivery, contractual, financial, tax, compliance, security, audit, dispute-resolution and legal record-keeping requirements.

Retention is category-based rather than a single blanket period. In particular:

- core commercial, financial, contractual, compliance and audit records may be retained for the period required by applicable law and CPC's legitimate record-keeping obligations;
- legal-acceptance and consent records may be retained to evidence what terms/policies applied and when;
- security and access logs are retained for an appropriate security/audit period based on risk and operational need;
- marketing consent, unsubscribe and suppression records may be retained as necessary to prove consent or continue honouring an opt-out;
- superseded or archived NPO documents may be retained where they form part of a transaction, compliance, protected-change, security or audit history;
- information in backups may persist for the applicable backup-retention cycle even after deletion from the live system.

When information is no longer required and CPC is legally permitted to remove it, CPC may securely delete it, de-identify it or destroy the relevant record through a controlled process. A deletion request does not require CPC to erase information that lawfully must or may be retained.

18. Data-subject rights

Subject to POPIA and other applicable law, a data subject may have the right to:

- request confirmation of whether CPC holds personal information about them and request access to it;
- request correction or updating of inaccurate, irrelevant, excessive, outdated, incomplete, misleading or unlawfully obtained information;
- request deletion or destruction where CPC is not lawfully entitled or required to retain the information;
- object, on reasonable grounds and where applicable, to certain processing;
- withdraw consent where processing is based on consent, without affecting prior lawful processing;
- object to direct marketing and unsubscribe from applicable marketing communications at any time;
- lodge a complaint with the Information Regulator.

CPC may need to verify identity and authority before acting on a request. Requests may be refused or limited where permitted by law, for example where disclosure would unlawfully affect another person, prejudice security, or conflict with a lawful retention obligation.

Requests can be submitted to the Information Officer using the contact details in section 2.

19. PAIA and access to records

Access to records may also be governed by the Promotion of Access to Information Act, 2000 (PAIA). Requests for records under PAIA must follow the applicable statutory process and may be subject to permitted grounds of refusal, fees and identity/authority verification.

CPC's PAIA Manual, where required/applicable, will be made available through CPC's website or from the Information Officer.

20. Third-party websites, services and external authorities

CPC websites or applications may link to third-party websites, payment pages, government resources or external services. CPC does not control the privacy practices of independent third parties. Users should review the privacy notice of the relevant third party before providing information directly to it.

Where CPC provides links or information relating to DSD, the Information Regulator, a municipality, government department or another authority, that authority remains independently responsible for its own systems and privacy practices.

21. Project-specific processing

CPC may undertake consulting, software, government, municipal, NPO or other client projects outside the CPC NPO Platform. Where a project requires personal information processing, CPC will determine whether it acts as responsible party, joint responsible party or operator, and will apply appropriate project-specific contractual, access, security, retention and confidentiality controls.

Where a client instructs CPC to process personal information on the client's behalf, the client remains responsible for ensuring that its instructions and the underlying collection/use of the information are lawful. CPC will process such information only within the agreed scope and documented instructions, subject to applicable legal obligations.

22. Changes to this policy

CPC may update this policy when legal requirements, providers, systems, projects or processing activities change. Material changes will be reflected by updating the version/effective date and, where appropriate, by providing additional notice or obtaining fresh consent where legally required.

Historical policy/acceptance records may be retained where necessary to establish which version applied to a user or transaction.

23. Complaints and the Information Regulator

If you have a concern about CPC's handling of personal information, please contact the CPC Information Officer first so that the matter can be investigated and, where appropriate, corrected.

You also have the right to complain to the Information Regulator (South Africa):

- Telephone: 010 023 5200
- Toll-free: 0800 017 160
- General enquiries: enquiries@inforegulator.org.za
- POPIA complaints: POPIAComplaints@inforegulator.org.za
- PAIA complaints: PAIAComplaints@inforegulator.org.za
- Physical address: Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, South Africa

Website / eServices: https://inforegulator.org.za | https://eservices.inforegulator.org.za

24. Contact CPC

Privacy, POPIA, PAIA and personal-information requests may be directed to:

- Castor Project Consultants (Pty) Ltd
- Information Officer: Stephan Haupt
- Email: stephan@castorprojects.com or info@castorprojects.com
- Address: 27 Outeniqua Street, Noordheuwel, Krugersdorp, 1739, South Africa
- Telephone: +27 81 645 9338

Website: https://castorprojects.com | Secure NPO application: https://npoapp.castorprojects.com

Document control note: This policy is drafted for CPC's current Phase 1A platform and broader CPC activities. Provider names, platform capabilities and processing practices must be reviewed before publication whenever the Production stack materially changes.