

DARK WATER OPS

(PTY) LTD

PRIVACY POLICY

Website and Service Information Protection Notice

CONFIDENTIAL | PROFESSIONAL | RESPONSIBLE

Effective date: 29 July 2026

Version 2.0

1. Purpose and Scope

Dark Water Ops (Pty) Ltd ("Dark Water Ops", "we", "us" or "our") respects privacy and is committed to processing personal information lawfully, reasonably and transparently. This policy explains how we collect, use, store, disclose and protect personal information in accordance with the Protection of Personal Information Act 4 of 2013 ("POPIA") and other applicable South African law.

This policy applies to personal information processed through www.darkwaterco.co.za, email, telephone, social media, forms, consultations, site visits, service instructions and operational activities. It covers clients, prospective clients, suppliers, contractors, subcontractors, employees, job applicants, website visitors, debtors, witnesses, subjects of lawful investigations, data appearing in due diligence work, and other people whose information is processed for a legitimate and lawful purpose.

It applies across Dark Water Ops services, including private investigations, VIP protection, tracking and tracing, debt recovery, information and evidence gathering, due diligence transparency reports, contractor and construction-site investigative audits, death-scene cleanup coordination and Dark Water Construction consulting activities.

Important

This policy governs privacy and personal-information processing. It does not replace a signed service agreement, confidentiality undertaking, investigation mandate, quotation, construction contract, website terms of use or any legal obligation. No policy can remove all business or legal risk, and Dark Water Ops will apply this policy together with the terms governing each instruction.

1.1 Responsible Party and Contact

Dark Water Ops (Pty) Ltd is the responsible party where it determines why and how personal information is processed. In some assignments, we may act as an operator for a client and process information only on that client's documented, lawful instructions.

Privacy contact / Information Officer	Dark Water Ops (Pty) Ltd
Email	darkwaterco@outlook.com
Website	www.darkwaterco.co.za

2. Key Definitions

- Data subject: the person or juristic person to whom personal information relates.
- Personal information: information relating to an identifiable living natural person and, where applicable, an identifiable existing juristic person, as defined by POPIA.
- Special personal information: information concerning matters such as health, race or ethnic origin, biometric information, trade-union membership, religious or philosophical beliefs, political persuasion, sex life or criminal behaviour.
- Processing: any operation involving personal information, including collection, recording, organisation, storage, updating, retrieval, consultation, use, sharing, restriction, erasure or destruction.
- Operator: a person who processes personal information for a responsible party under a mandate or contract, without being under that party's direct authority.

3. Information We May Process

The information processed depends on the service, instruction and lawful purpose. It may include:

- Identity and contact details, including names, identity or registration numbers, addresses, telephone numbers, email addresses and authorised representatives.
- Company, director, member, shareholder, employment, professional, supplier, contractor and subcontractor information.
- Financial, banking, billing, payment, debt, credit-related and transactional information where relevant and lawfully obtained.
- Service records, instructions, contracts, quotations, correspondence, call notes, complaints and consent or authority records.
- Investigation and verification information, including photographs, video, audio, statements, observations, public-record information, location or tracing data, case references and evidence records where lawfully processed.
- Security and protection information, including risk assessments, schedules, access arrangements, emergency contacts and incident records.
- Construction and site information, including site access records, contractor documentation, safety records, project communications, progress photographs, defects, incidents and verification results.
- Death-scene cleanup information that is strictly necessary for authorised coordination, safety, access, billing, service delivery and record-keeping.
- Website and device information, including IP address, browser type, device identifiers, pages viewed, date and time data, referring pages and cookie preferences.
- Special personal information or children's information only where lawful, necessary and subject to appropriate safeguards or authorisation.

3.1 Minimality and Accuracy

We aim to collect information that is adequate, relevant and not excessive for the identified purpose. We take reasonably practicable steps to keep information accurate, complete and not misleading, having regard to the purpose for which it is processed. Information from public or third-party sources may be verified where appropriate, but its accuracy cannot always be guaranteed.

4. How We Collect Information

We may obtain personal information:

- Directly from you, your authorised representative, a client, contractor, supplier, debtor, witness or service provider.
- Through forms, applications, instructions, agreements, calls, emails, meetings, site visits, interviews, statements and service interactions.
- From public records, public websites, social media, company records, regulatory sources, courts or other lawfully accessible sources.
- From credit bureaus, tracing providers, fraud-prevention services, professional advisers, law-enforcement bodies or other authorised third parties where permitted by law.
- Through lawful investigation, surveillance, evidence-gathering or verification activities carried out under an appropriate mandate and within applicable legal boundaries.
- Automatically through website logs, security tools and cookies or similar technologies.

Where information is not collected directly from the data subject, we will rely on a lawful basis and provide notification where POPIA requires it and no lawful exception applies.

5. Lawful Grounds for Processing

Depending on the circumstances, we process personal information because:

- the data subject has given valid consent;
- processing is necessary to conclude or perform a contract;
- processing complies with an obligation imposed by law;
- processing protects a legitimate interest of the data subject;
- processing is necessary for the proper performance of a public-law duty by a public body; or
- processing protects our legitimate interests or those of a third party, provided the processing remains lawful and reasonable.

Consent is not used as a blanket justification. Where consent is relied on, it may be withdrawn, but withdrawal does not invalidate prior lawful processing and does not prevent continued processing where another lawful ground applies.

6. Purposes for Which Information Is Used

We may process information for the following defined purposes:

- To assess enquiries, verify authority, provide quotations, open instructions and deliver contracted services.
- To plan and perform investigations, protection assignments, tracing, debt recovery, due diligence, evidence gathering, audits, cleanup coordination and construction consulting.
- To verify identity, company status, authority, ownership, credentials, references, banking details, operational standing and other relevant information.
- To communicate with clients and relevant parties, provide progress updates, respond to enquiries and manage complaints.
- To protect people, property, sites, evidence, systems, confidential information and legal rights.
- To maintain case files, audit trails, chain-of-custody records, service records, financial records and legally required documentation.
- To invoice, collect payment, administer accounts, recover lawful debts and prevent fraud or misuse.
- To establish, exercise or defend legal claims; comply with subpoenas, court orders, lawful requests and regulatory duties; and cooperate with authorised authorities.
- To manage suppliers, operators, contractors, subcontractors, professional advisers and business continuity.
- To secure, maintain and improve our website, systems, services, training, quality controls and risk management.
- To send marketing communications where permitted by law and to honour objections or opt-out requests.

7. Service-Specific Privacy Safeguards

7.1 Investigations, Tracking, Tracing and Evidence

Investigation-related information may be sensitive and confidential. We process it only for a lawful, defined instruction or other lawful purpose. Access is limited to personnel and service providers who require it. Investigation findings reflect information available at the time and may include allegations or unverified third-party information, which will be identified as such where reasonably practicable.

We do not publish investigation material merely because we possess it. Disclosure is limited to authorised clients, legal representatives, courts, regulators, law-enforcement bodies or other recipients where lawful and necessary. No person may use our reports or evidence for harassment, unlawful discrimination, intimidation or any purpose outside the agreed mandate.

7.2 Due Diligence and Contractor Verification

Due diligence transparency reports and contractor verifications may draw on supplied documentation, public records and lawfully obtained third-party information. Reports are prepared for the requesting client's defined decision-making purpose and must not be treated as a guarantee of future conduct, financial performance or project success. Recipients must keep reports confidential and use them only for the authorised purpose.

7.3 Debt Recovery

For lawful debt-recovery instructions, we may process debtor identity, contact, account, communication, payment and tracing information. We require clients to confirm their authority and the basis of the debt. Information may be shared with authorised collection personnel, legal advisers, tracing providers, credit-related service providers, courts or regulators only where lawful and necessary. A disputed debt will be recorded and handled according to the applicable process.

7.4 VIP Protection and Security Services

Protection assignments may require sensitive schedules, locations, travel arrangements, access details, emergency contacts and risk assessments. Such information is restricted on a need-to-know basis and should not be shared by clients or third parties without authorisation.

7.5 Construction Consulting and Site Activities

Construction-related processing may include contractor, employee, visitor, site-access, safety, incident, project and photographic records. Information is used for consulting, verification, audit, security, safety, contract administration, dispute management and project documentation. Clients remain responsible for ensuring that they have authority to provide employee, contractor or site information to us.

7.6 Death-Scene Cleanup

Information connected to death-scene cleanup is handled with heightened sensitivity, dignity and discretion. We limit processing to what is necessary for lawful authorisation, access, risk and safety management, service coordination, billing, regulatory obligations and incident documentation. Images or sensitive details are not used for marketing without a separate lawful basis and explicit written authority where required.

8. Special Personal Information and Children

We do not rely on a general statement of consent to process special personal information or children's information. We process such information only where POPIA permits it, where the required consent or authorisation exists, or where another lawful exception applies. Additional access restrictions, confidentiality controls and retention limits may apply.

Our website and general services are not directed at children. A person under 18 should not submit information or request services without the involvement of a parent, guardian or other competent person. If you provide information about a child, you confirm that you are authorised to do so.

9. Sharing and Disclosure

We do not sell personal information. We may disclose it only where lawful and reasonably necessary to:

- the data subject, an authorised representative or the client who lawfully instructed the processing;
- employees, investigators, protection personnel, consultants and authorised internal personnel on a need-to-know basis;
- operators and service providers, including secure hosting, communications, payment, IT, tracing, verification, professional and records-management providers;
- legal advisers, insurers, auditors, accountants, experts, contractors and subcontractors subject to appropriate duties;
- credit bureaus, fraud-prevention bodies or collection-related providers where the law and the instruction permit;
- courts, tribunals, regulators, law-enforcement bodies or public authorities in response to a lawful request or duty;
- a successor or purchaser in a genuine business transaction, subject to confidentiality and lawful processing requirements.

Operators are required, through appropriate contractual or other safeguards, to process information only for authorised purposes, maintain confidentiality and implement reasonable security measures.

10. Cross-Border Processing

Personal information may be stored or processed outside South Africa only where permitted by POPIA. We will use a lawful transfer mechanism, which may include adequate legal protection in the recipient country, a binding agreement providing an adequate level of protection, data-subject consent where appropriate, or another basis allowed by law. We do not treat use of the website as blanket consent to every cross-border transfer.

11. Information Security and Confidentiality

We implement reasonable technical and organisational safeguards appropriate to the nature of the information and the risks involved. Measures may include access controls, authentication, device and network safeguards, secure storage, confidentiality duties, personnel controls, backups, incident procedures, controlled sharing and secure disposal. Access is limited according to role and operational need.

No method of internet transmission or electronic storage is completely secure. We cannot promise absolute security, but we will take reasonably practicable steps required by law. Clients and users must protect their passwords, devices and communications and must promptly report suspected unauthorised access.

11.1 Security Compromises

Where there are reasonable grounds to believe that personal information has been accessed or acquired by an unauthorised person, we will investigate, contain and assess the incident and notify the Information Regulator and affected data subjects as required by POPIA, subject to any lawful delay or exception.

12. Retention and Destruction

We retain personal information only for as long as necessary for the purpose for which it was collected, as required by law, under a contract or mandate, or for the establishment, exercise or defence of legal claims. Retention periods may differ for financial records, case files, evidence, investigation records, debt-recovery records, due diligence reports, construction documentation, security incidents and website logs.

When information is no longer required and no lawful reason for retention remains, it will be destroyed, deleted or de-identified in a manner intended to prevent reconstruction. A legal hold, dispute, investigation, regulatory process or client instruction may temporarily suspend ordinary deletion.

13. Cookies and Website Analytics

Our website may use essential cookies and similar technologies for security, functionality, preferences and basic traffic analysis. Non-essential cookies should be used only with an appropriate choice mechanism where required. You may change browser settings or cookie preferences, but blocking essential cookies may affect website functionality.

If third-party analytics, embedded content, maps, videos or social-media tools are introduced, those providers may process information under their own privacy notices. We will identify material third-party tools through the website or cookie notice where reasonably practicable.

14. Direct Marketing

We conduct electronic direct marketing only as permitted by POPIA. Where consent is required, we will request it in the prescribed or otherwise lawful manner. Existing clients may receive communications about similar services where the law permits. Every marketing communication will provide a reasonable way to opt out, and objections will be recorded.

15. Your Rights

Subject to POPIA and any applicable limitation, a data subject may:

- ask whether we hold personal information about them and request access to it;
- request correction, completion, updating, deletion or destruction of inaccurate, irrelevant, excessive, outdated, incomplete, misleading or unlawfully obtained information;
- object, on reasonable grounds, to certain processing or object to direct marketing at any time;
- withdraw consent where processing is based on consent;
- request information about the identity of third parties who have had access where POPIA provides for it;
- complain to us or lodge a complaint with the Information Regulator;
- challenge a decision based solely on automated processing where POPIA applies.

Requests must be sent to darkwaterco@outlook.com. We may request proof of identity and authority before acting, and we may refuse or limit a request where the law permits or requires it. Any prescribed fee or access procedure will be explained before the request is completed.

16. Third-Party Links and Platforms

Our website or communications may link to third-party websites, social-media pages, portals or services. Their privacy practices are controlled by their own operators. We are not responsible for their content, security or processing merely because a link is provided. Users should review the relevant third-party privacy notice before submitting information.

17. Accuracy of Client-Supplied Information and Authority

A client or third party who supplies personal information to us confirms that they are authorised to do so, that the instruction is lawful, and that the information is not knowingly false or misleading. Dark Water Ops may request proof of authority, consent, mandate, debt, identity or other supporting documentation and may decline or suspend an instruction where legality, authority or accuracy is reasonably in doubt.

The client remains responsible for its own POPIA duties where it determines the purpose and means of processing. Nothing in this policy transfers a client's legal obligations to Dark Water Ops.

18. Changes to This Policy

We may amend this policy to reflect legal, regulatory, operational or service changes. The current version will be published on our website with its effective date. Material changes may be communicated through the website or another appropriate channel. Continued use of the website does not create consent where POPIA requires a separate lawful basis.

19. Complaints and Information Regulator

Please first contact our Privacy Contact at darkwaterco@outlook.com so that we can assess and address the concern. You may also lodge a complaint with the Information Regulator (South Africa):

Website	www.inforegulator.org.za
POPIA complaints	POPIAComplaints@inforegulator.org.za
General enquiries	enquiries@inforegulator.org.za
Telephone	010 023 5200 Toll free: 0800 017 160
Address	Woodmead North Office Park, 54 Maxwell Drive, Woodmead, Johannesburg, 2191

Document status

This policy is intended as a professional operational privacy notice for the Dark Water Ops website and services. It should be reviewed by a qualified South African legal professional and updated when business processes, operators, cookies, service offerings or applicable laws change.

Approved for publication by Dark Water Ops (Pty) Ltd.

Effective date: 29 July 2026

Version: 2.0