



Privacy Policy: Aboriginal Data Sovereignty and Free, Prior and Informed Consent

Effective date: 5 August 2026

Privacy | Aboriginal Data Sovereignty | Indigenous Data Governance | FPIC

1. Our commitment

Black Wattle Professional Services Pty Ltd ACN: 699 642 969 and ABN: 64 699 642 969 (Black Wattle, we, us or our) is committed to respecting privacy and handling personal information and Aboriginal Data responsibly, transparently and with cultural care.

We use the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs) as the benchmark for our privacy practices to the extent they apply to us. We also comply with applicable contractual, professional and legal obligations.

As a 100% Aboriginal-owned consultancy, Black Wattle recognises that information about Aboriginal and Torres Strait Islander peoples is not simply a business asset or an individual record. It may be culturally sensitive, collectively held, connected to Country, governed by cultural authority and subject to responsibilities to families, communities and future generations.

Our approach is informed by:

- the right of Aboriginal and Torres Strait Islander peoples to self-determination;
- Aboriginal and Torres Strait Islander leadership and decision-making authority;
- Aboriginal Data Sovereignty and Indigenous Data Governance;
- Free, Prior and Informed Consent (FPIC);
- the United Nations Declaration on the Rights of Indigenous Peoples (UNDRIP);
- the AIATSIS Code of Ethics for Aboriginal and Torres Strait Islander Research; and
- applicable community protocols, cultural authority and Indigenous Cultural and Intellectual Property rights.

This statement explains how we collect, create, hold, govern, access, analyse, interpret, use, disclose, publish, retain, return and dispose of personal information and Aboriginal Data in connection with our website and services.

2. What we mean by Aboriginal Data

In this statement, **Aboriginal Data** means information, knowledge or material, in any format, that is about, relates to, is created by, or may affect Aboriginal and Torres Strait Islander individuals, families, communities, organisations, peoples, cultures, languages, Countries, lands, waters, resources or knowledges.

Aboriginal Data may include:

- personal and sensitive information;
- community-level, organisational and administrative information;
- research, evaluation, survey, consultation and engagement data;
- stories, oral histories, cultural knowledge and community perspectives;
- photographs, artwork, audio, video and other recordings;
- cultural heritage, language, Country and place-based information;
- workforce, recruitment, health, education, service-delivery and demographic information;
- reports, analysis, interpretations, statistics and data visualisations; and

- metadata, linked data, de-identified data and aggregated data where Aboriginal people or communities may still be identifiable or affected.

Aboriginal Data may have collective significance even when it does not meet the legal definition of personal information.

3. Aboriginal Data Sovereignty

Black Wattle recognises Aboriginal Data Sovereignty as the right of Aboriginal and Torres Strait Islander peoples to govern data about their peoples, communities, cultures, Countries and resources, regardless of where that data is held or who holds it.

Where Black Wattle handles Aboriginal Data, we will seek to support the rights of the relevant Aboriginal and Torres Strait Islander people, community or organisation to exercise authority over:

- why and how data is created or collected;
- who owns, controls, holds and is accountable for the data;
- where and how data is stored and protected;
- who may access the data and under what conditions;
- how data is classified, linked, analysed and interpreted;
- how findings are validated, attributed, communicated and published;
- whether data may be shared, licensed, commercialised or reused;
- how benefits arising from the data are identified and shared;
- how data supports community priorities, capability and self-determination; and
- when data is retained, returned, archived, transferred, de-identified or destroyed.

Black Wattle will not assume that holding Aboriginal Data gives us ownership, unrestricted control or an ongoing right to use it.

4. Our Aboriginal Data Governance principles

When our work involves Aboriginal Data, we will apply the following principles proportionately to the nature, sensitivity and potential impact of the data.

Self-determination and Aboriginal leadership

Aboriginal and Torres Strait Islander peoples should be involved in decisions about data that relates to or affects them. We will seek to identify and engage the people or bodies with the appropriate cultural, community or organisational authority.

Collective and individual rights

We recognise that privacy law generally protects individuals, while Aboriginal Data Sovereignty also recognises collective rights and interests. Individual consent does not automatically replace the need for community authority, and community authorisation does not remove an individual's privacy rights or right to choose whether to participate.

Purpose limitation and data minimisation

We will seek to collect or create only the data reasonably required for an agreed purpose. Data will not be used for a new or unrelated purpose without further authority, consent or another lawful basis.

Cultural safety and contextual integrity

Data will be interpreted and presented with appropriate cultural, historical, social and community context. We will seek to avoid deficit framing, stereotyping, stigmatisation, inaccurate comparison, harmful aggregation or conclusions that could misrepresent Aboriginal and Torres Strait Islander peoples.

Community benefit and reciprocity

Where appropriate, we will discuss how the work and its data can provide meaningful benefit to the relevant people or community. This may include access to findings, community-owned outputs, capability strengthening, knowledge exchange, appropriate recognition or other agreed benefits.

Transparency and accountability

We will seek to make data arrangements understandable and document important decisions, permissions, restrictions and responsibilities. We will provide appropriate ways for people and communities to raise concerns and seek review.

Access, return and continuing stewardship

Where appropriate, we will plan how the relevant Aboriginal and Torres Strait Islander people, community or organisation can access, use, receive or retain their data and project outputs beyond the life of a project.

5. Free, Prior and Informed Consent

Black Wattle uses FPIC as a core standard when proposed work may collect, create, use, disclose or publish Aboriginal Data or may affect the rights, interests, knowledge or priorities of Aboriginal and Torres Strait Islander peoples.

FPIC means that consent should be:

- **Free:** given voluntarily, without coercion, manipulation, intimidation, pressure or an unreasonable disadvantage for declining;
- **Prior:** sought sufficiently before collection, engagement, a decision or activity begins, allowing time for cultural and community decision-making processes;
- **Informed:** based on clear, accessible and culturally appropriate information about the activity, purpose, methods, risks, benefits, participants, data arrangements, potential uses, disclosures, outputs, funding and any commercial interests; and
- **Consent:** an affirmative and continuing agreement given through the decision-making process chosen by the relevant Aboriginal and Torres Strait Islander people, community or

organisation. Consent may be granted, subject to conditions, withheld, reviewed, renegotiated or withdrawn.

FPIC is a continuing relationship and process, not merely a signature or one-time transaction. The form of consent may be written, verbal, recorded or provided through another agreed culturally appropriate process. We will seek to document the outcome and any conditions without imposing an inappropriate process.

Before relevant work begins, we will seek to clarify:

- who has authority to speak for or make decisions about the people, community, Country, knowledge or data involved;
- who should participate in the decision and how much time is required;
- the scope and purpose of the activity;
- what data will be collected or created and whether any participation is optional;
- who will own, hold, access, analyse and interpret the data;
- proposed uses, disclosures, publications and outputs;
- whether data may be stored overseas or accessed by technology providers;
- reasonably foreseeable risks and intended benefits;
- how consent can be reviewed, limited or withdrawn;
- what will happen to data already collected if consent is withdrawn; and
- how disputes, changes in scope and unexpected findings will be managed.

Where the purpose, scope, technology, project partners, risks or proposed uses materially change, we will pause the affected activity and seek renewed consent or authority before proceeding.

Withdrawing consent will apply to future handling where reasonably practicable. We will explain any legal, contractual, safety, evidentiary or practical limits on removing information already incorporated into completed or published outputs.

6. What personal information we may collect

Depending on how you interact with us, we may collect:

- your name, pronouns, contact details, location, organisation, position and professional details;
- correspondence, enquiries, feedback, complaints and communication preferences;
- information provided through meetings, interviews, surveys, workshops, consultations, evaluations and engagement activities;
- photographs, artwork, audio or video recordings where appropriate permission has been obtained;
- client, supplier, contractor, invoicing and payment information;
- website information, such as your IP address, browser or device information, pages visited, cookies and information submitted through online forms; and

- recruitment information, including a resume, qualifications, employment history, professional memberships, interview and assessment information, referee details, work eligibility, remuneration expectations and relevant background or probity checks.

We may also collect sensitive information where it is reasonably necessary for our work and the required consent or authority has been obtained, or where collection is otherwise permitted or required by law. This may include information about:

- Aboriginal or Torres Strait Islander identity, racial or ethnic origin, cultural identity, language group, family, kinship, community connections or affiliations;
- health, disability or accessibility requirements;
- criminal history or other probity information relevant to a position; and
- other cultural, demographic or personal information voluntarily shared during research, evaluation, recruitment or engagement activities.

7. How we collect information and Aboriginal Data

We usually collect information directly from you when you:

- contact us by email, telephone, our website or social media;
- engage us or participate in a project, meeting, consultation, workshop, survey, interview, evaluation or training activity;
- apply for a position or participate in a recruitment process;
- subscribe to updates or register for an event; or
- work with us as a client, consultant, contractor, supplier or community partner.

We may also receive information from an authorised representative, client organisation, Traditional Owner body, community-controlled organisation, referee, recruitment platform, screening provider, project partner or publicly available professional source.

Where reasonable and appropriate, we will provide a privacy notice, participant information or data governance information before or when information is collected. For projects involving material Aboriginal Data, this may include an agreed consent protocol, data governance plan, research agreement or project-specific information statement.

You may interact with us anonymously or use a pseudonym where this is lawful and practical. In some circumstances, however, we may be unable to provide a service, progress an application or respond fully without identifying information.

8. Why we collect and use information

We may collect, create, hold, analyse, use and disclose information to:

- respond to enquiries and communicate with you;
- scope, plan, manage and deliver consulting services and projects;
- conduct research, evaluation, stakeholder engagement and community consultation;
- design and deliver workshops, training, mentoring and events;

- conduct recruitment, executive search, candidate assessment, reference checking, due diligence, appointment and onboarding processes;
- manage client, consultant, contractor, supplier and professional relationships;
- prepare contracts, invoices, reports and other business records;
- administer our website, mailing list and events;
- improve our services, quality, accessibility and cultural responsiveness;
- maintain security, manage risk and protect lawful interests; and
- meet legal, regulatory, insurance, audit and contractual obligations.

We will not use personal information or Aboriginal Data for a materially different purpose unless the appropriate individual consent, community or organisational authority, and lawful basis have been obtained.

9. Project-specific Aboriginal Data Governance

Where warranted by the nature of a project, Black Wattle will work with the relevant client, Aboriginal and Torres Strait Islander people, community or organisation to establish proportionate data governance arrangements covering matters such as:

- purpose, priorities and expected community benefit;
- leadership, decision-making authority and governance roles;
- ownership, custodianship, control and intellectual property;
- collection methods and participant consent;
- cultural restrictions, confidentiality and authorised access;
- data location, security and approved technology;
- analysis, interpretation and community validation;
- publication, attribution, acknowledgement and communication;
- third-party access, sharing, linkage and secondary use;
- commercial use, licensing and benefit-sharing;
- correction, withdrawal and dispute resolution; and
- retention, community access, return, archiving and destruction.

De-identifying data does not automatically remove cultural, collective or community risks. We will consider whether individuals, families, communities, organisations or places could be identified or harmed through context, small numbers, linked datasets or the subject matter.

We will not make Aboriginal Data publicly available or treat it as open data solely because direct personal identifiers have been removed.

We will not use identifiable, confidential, culturally restricted or culturally sensitive Aboriginal Data to train an artificial intelligence model, or enter it into a public or externally controlled generative AI system, without explicit and specific authorisation and agreed safeguards.

10. Recruitment information

When Black Wattle conducts recruitment or executive search work, we may handle personal information for, or jointly with, a client organisation. We will explain the relevant process and seek permission before presenting identifiable candidate information to a client, except where disclosure is otherwise authorised or required by law.

Information about a person's Aboriginal or Torres Strait Islander identity will be handled as sensitive information. Where identity is relevant to an identified position or culturally responsive recruitment process, we will explain why the information is requested, how it may be assessed or verified and who may receive it.

Candidate information is used for the relevant recruitment process and associated due diligence. If we wish to retain a candidate's details for future opportunities, we will provide notice and an opportunity to decline or later withdraw that permission.

We do not make recruitment or other decisions that significantly affect a person solely through automated processing. Technology may assist administrative work, but material decisions remain subject to human review and professional judgement.

11. When we disclose information

We may disclose personal information or Aboriginal Data, only where appropriate and within the scope of applicable consent, cultural authority, data governance arrangements, contract and law, to:

- Black Wattle personnel and authorised consultants or contractors who need it to perform their work;
- client organisations involved in an agreed project or recruitment process;
- referees, screening services or professional advisers involved in authorised verification and due diligence;
- trusted providers supporting our website, cloud storage, email, communications, accounting, payment, document management, event management, analytics, cybersecurity or other business systems;
- project partners, facilitators, cultural advisers or community representatives where this has been explained and authorised;
- insurers, auditors, accountants, lawyers and other professional advisers; and
- courts, regulators, law enforcement agencies or government authorities where disclosure is required or authorised by law.

Where a contractor or provider handles Aboriginal Data for us, we will seek to communicate relevant restrictions and require protections appropriate to the sensitivity and cultural significance of the data.

We do not sell, rent or trade personal information, Aboriginal Data or community contact lists.

Where we process information on behalf of a client, the client's privacy policy, its data governance responsibilities and our contractual obligations may also apply. Black Wattle will raise concerns where a proposed client direction appears inconsistent with agreed consent, cultural authority or data governance arrangements.

12. Overseas storage and disclosure

Some third-party digital service providers may store or process information outside Australia, including in the United States. Provider locations can change depending on the service and its infrastructure.

Where an overseas disclosure is likely, we will take reasonable steps appropriate to the circumstances to protect the information and comply with applicable privacy obligations.

Where Aboriginal Data is likely to be stored, accessed or disclosed overseas, we will seek to address this in the relevant notice, FPIC process or data governance arrangement, including any material risks, safeguards and available alternatives.

13. Website, cookies and third-party services

Our website may use cookies and similar technologies to support site functionality, understand aggregated website traffic and improve user experience. You can control or disable cookies through your browser settings, although this may affect some website functions.

Our website contact form uses Google reCAPTCHA to reduce spam and misuse. Google's Privacy Policy and Terms of Service may apply when you use that form.

Our website may also contain links to third-party websites. We are not responsible for the privacy practices of those third parties and encourage you to review their privacy policies.

14. Direct communications and marketing

We may send updates about our services, training or opportunities where you have asked to receive them or where otherwise permitted by law. You can unsubscribe at any time by using the unsubscribe option in the communication or contacting us.

We will not use sensitive information, cultural information, community contact details, stories, images or recordings for marketing without the specific permission and cultural authority required for that use.

15. How we protect information

We take reasonable administrative, technical, physical and culturally informed steps to protect personal information and Aboriginal Data from misuse, interference, loss and unauthorised access, modification, disclosure or culturally inappropriate use.

These measures may include access controls, secure systems, confidentiality obligations, staff and contractor requirements, separating or restricting sensitive records, documenting cultural restrictions, and limiting access to people who need the information for an authorised purpose.

No method of electronic transmission or storage is completely secure. If a data breach occurs, we will take reasonable steps to contain and assess it and will notify affected individuals and the Office of the Australian Information Commissioner where required by law.

Where a breach involves Aboriginal Data, we will also consider collective, cultural and community harm and, where appropriate, engage the authorised community or organisational representatives about containment, notification, remedy and prevention.

16. Retention, return and disposal

We retain personal information and Aboriginal Data only for as long as reasonably necessary for the agreed purpose and to meet legal, contractual, insurance and legitimate recordkeeping requirements.

For Aboriginal Data, retention and disposal decisions may also be governed by cultural authority, Indigenous Cultural and Intellectual Property rights and project-specific data governance arrangements. Depending on what has been agreed, we may return or transfer data to an authorised community-controlled repository, support continuing community access, retain it subject to agreed restrictions, or securely destroy it.

We will not retain Aboriginal Data indefinitely merely because it may be useful for an unspecified future purpose.

17. Access, correction and withdrawal

You may ask to:

- access personal information we hold about you;
- correct information that is inaccurate, incomplete, out-of-date, irrelevant or misleading;
- withdraw a consent previously provided, subject to applicable limits;
- ask how your information has been used or disclosed; or
- raise concerns about cultural restrictions or the handling of Aboriginal Data.

An authorised Aboriginal and Torres Strait Islander community or organisation may also contact us about access to, correction of, governance of or restrictions applying to Aboriginal Data relating to it. We will consider the request in light of cultural authority, individual privacy, existing agreements, intellectual property, confidentiality and applicable law.

We may ask you to verify your identity or authority before responding. In limited circumstances, the law or the rights of another person may require us to refuse or limit a request. If that occurs, we will explain our decision where we are able to do so.

18. Privacy and Aboriginal Data concerns or complaints

If you have a privacy, FPIC or Aboriginal Data Governance question, concern or complaint, please contact us and include enough information for us to understand the issue.

We will acknowledge the matter, investigate it fairly and aim to provide a response within 30 days. Where a matter involves collective rights, cultural authority or community harm, we may discuss an appropriate resolution process with the relevant people or representatives. This may include culturally appropriate dialogue, correction, restricted access, removal from future use, return, additional safeguards or another agreed remedy.

If you are not satisfied with our response and the *Privacy Act 1988* applies to the matter, you may contact the Office of the Australian Information Commissioner at www.oaic.gov.au or by telephone on 1300 363 992.

19. Changes to this statement

We may update this statement when our practices, services, technology, guidance or legal obligations change.

Where a proposed change would materially affect an existing agreed use of Aboriginal Data, publication, disclosure or data governance arrangement, we will not rely solely on a general website update. We will seek renewed consent or authority where required by the relevant FPIC process, agreement or law.

The current version of this statement will be published on our website and will show its effective date.

20. Contact us

Privacy and Aboriginal Data Governance Contact

Black Wattle Professional Services Pty Ltd

Email: projects@blackwattleps.com.au

Website: www.blackwattleps.com.au