Laterite's AI Use Policy

October 2025

laterite

DATA | RESEARCH | ANALYTICS

Laterite's AI Use Policy

At Laterite, we embrace innovation in all its forms – including the responsible use of Artificial Intelligence (AI). As a research firm, we recognize AI's potential to enhance our productivity, improve data processing, and support analytical rigor. However, we also understand that using AI responsibly requires careful oversight, transparency, and respect for privacy.

This policy applies to all Laterite staff, contractors, and affiliates, and guides how we select tools, process data, and communicate with clients. It lays out our principles, practices, and safeguards for using AI across our work.

> 📌 Given the rapidly evolving AI landscape, this is a living document that will be updated regularly as new technologies, best practices, and regulatory frameworks emerge.
>
> Last update: October 27, 2025

Our Approach to AI

At the heart of our AI strategy is trust in our people. We encourage our team to use their best judgment when working with AI tools. While this policy provides guardrails, we recognize that responsible decision-making often depends on context. We trust our team to balance efficiency, quality, and ethical considerations in every instance.

We encourage the use of AI tools to support and accelerate our work. These tools can assist with drafting reports, transcribing interviews, summarizing literature, coding data, and more.

However, AI is never a substitute for expert judgment. Every AI output must be reviewed, verified, and refined by a qualified human before it's shared externally or used in decision-making. We do not copy-paste from AI without multiple iterations and human review/guidance. We never rely on it to produce final outputs. Instead, we treat it as a co-pilot - useful, but never in charge. Any reviewed AI output that will be used in client-facing outputs must come together with our AI Usage Disclaimer (see "Communicating with Clients" section below).

✅ **We permit the use of approved AI tools for tasks such as:**

- Writing, debugging, or improving code in Python, R, Stata, SurveyCTO, etc.
- Transcribing or translating anonymized audio or documents, with consent[1]
- Thematic coding of anonymized qualitative data
- Conducting "Deep Research" searches and literature reviews
- Improving the clarity, structure, and quality of written outputs
- Supporting learning, ideation, and brainstorming processes
- Drafting summaries or outlines of lengthy documents (e.g., program documents, policies, terms of reference) for ease of internal review
- Suggesting analytical approaches, flagged for expert validation

❌ **We do not allow:**

- Uploading identifiable or sensitive data to AI tools, unless we have consent or are using pre-approved enterprise tools
- Using AI outputs without human oversight
- Letting external AI providers retain or use our data
- Deploying AI outputs as-is in reports, proposals, or policy recommendations

Privacy and Data Protection

Protecting the privacy of research participants, our clients, and Laterite staff is central to everything we do. That principle extends fully to our use of AI:

- We never feed Personally Identifiable Information (PII) into AI systems. This includes names, phone numbers, addresses, or any information that might identify an individual, including research participants, Laterite staff, or our clients and partners.
- All data must be anonymized before it's processed.
- We only use AI tools that are pre-approved by Laterite, which means they have been vetted for data security and do not retain or train on our data. Currently, this pre-approved list includes:

[1] Transcribing and translating must go through LateriteAI or other pre-approved tools. When in doubt, please reach out to the Analytics team.

  - Google Gemini (must be accessed through your Laterite enterprise account), including enterprise integration with Google Drive and Gmail
  - OpenAI ChatGPT (ensuring you have opted out of sharing data for model training, or are using a Laterite enterprise account), including enterprise integration tools with Google products
  - Anthropic Claude (ensuring you have opted out of sharing data for model training)
  - LateriteAI accessed via Slack

Audio data, in particular, deserves special care. Since voice recordings are considered biometric data under privacy regulations like the EU GDPR, we only process them through LateriteAI or another pre-approved tool. We also ensure that consent is properly documented - specifically covering the use of automated transcription and that any country specific data protection requirements are taken into consideration.

Laterite's internally developed AI tools, including LateriteAI, must adhere to the same principles. These internal models are developed and trained using publicly available data or using data for which Laterite has been given consent to use for tool development. PII is never used in the development of these models. Any data shared with internal tools like LateriteAI is stored securely, and any external models called via API calls are not permitted to store the data.

Bias and Algorithmic Fairness

AI systems can perpetuate or amplify existing biases, and these tools sometimes reflect the biases present in their training data. Given our work across diverse cultural and linguistic backgrounds, it's important to be proactive in identifying potential sources of bias in our AI use.

Laterite staff should keep in mind that AI outputs may not always accurately represent different geographic regions, demographic groups, or cultural contexts. When relevant – for example, when using AI to classify themes in qualitative interview transcripts, conduct literature reviews, or suggest analytical approaches – test outputs for consistency across different populations or contexts. Team members familiar with local contexts and languages must review AI-assisted work, particularly when working with marginalized communities or underrepresented regions. Document and report instances where you notice potential bias or cultural insensitivity in AI outputs so we can learn and improve our practices over time.

Communicating with Clients

Transparency is non-negotiable. We disclose AI use at every major touchpoint:

- In our proposals, we explain that we use AI tools to support our work - always with human oversight and privacy safeguards.

- In our data processing agreements, we specify the categories of AI processing we undertake, the tools we use, and the measures we take to protect data.
- In our final deliverables, we include a short note about AI contributions (e.g. transcription, formatting assistance, translation), reaffirming that all outputs have been reviewed by our team. See the AI Usage Disclaimer in the box below.
- In the event a client is not comfortable with the use of AI for their project we must provide options to complete the work without the use of AI tools.

AI Usage Disclaimer

As Artificial Intelligence (AI) capabilities advance at a rapid pace, Laterite is committed to staying at the cutting edge of this technology's potential to contribute to social good while maintaining high standards of ethics and quality. At Laterite, we may use AI tools to support and enhance our research processes, including tasks such as data transcription, analysis, and portions of report drafting. All AI-generated outputs are reviewed, verified, and refined by qualified team members with expertise in relevant subject matter and local context to ensure quality and accuracy.

We prioritize transparency and adhere to strict privacy safeguards, ensuring that no Personally Identifiable Information (PII) is processed by AI systems. We use only pre-approved AI tools that do not retain or train on our data. AI is never used as a substitute for expert judgment, and all final deliverables reflect the expertise and oversight of our team.

For more information on our AI usage practices, please refer to our internal AI policy.

Governance and Oversight

We have clear roles and responsibilities to ensure AI is used safely and effectively:

- Every project has a project lead who is responsible for the quality of the output and ultimately the use of AI in this assignment.
- The Analytics Team maintains our list of approved tools and reviews new ones before use.
- The Data Protection Officer (DPO) oversees how we handle personal data, including audio and biometric information.
- We require staff to join all training sessions on responsible AI use.

Risks and Incident Response

We recognize that AI use introduces new risks to our research quality, participant safety, and organizational reputation. We maintain robust procedures to identify, assess, and respond to AI-related incidents.

Risk categories we monitor:

- Research quality risks: AI errors affecting data analysis, coding accuracy, or analytical conclusions
- Participant safety risks: AI-assisted processes that could expose participants to harm or privacy violations
- Cultural sensitivity risks: AI outputs that misrepresent or stereotype the communities we work with
- Technical risks: System failures, data breaches, or unauthorized access to AI-processed information
- Bias risks: Systematic errors that disadvantage certain populations or geographic regions

Incident response procedures: When AI-related incidents occur, we follow a structured response:

1. Immediate response: The project lead stops use of the affected AI tool and assesses potential harm to participants or research quality
2. Documentation: All incidents are reported to the Analytics Team and DPO within 24 hours with details of what occurred and initial impact assessment
3. Investigation: The Analytics Team investigates root causes and determines the scope of impact on current and past work
4. Remediation: We implement corrective measures, which may include:
    - Reprocessing affected data with human oversight
    - Contacting participants if their privacy or safety may have been compromised
    - Informing the country office data protection authority of the data breach
    - Revising AI-assisted analysis or recommendations
    - Updating our approved tools list or usage guidelines
5. Communication: We inform relevant clients about incidents that may affect research quality or deliverables, maintaining transparency about our AI use limitations
6. Learning: We update our AI usage guidelines and training materials based on lessons learned

Escalation criteria: Incidents requiring immediate escalation to senior leadership include:

- Any potential harm to research participants
- Significant bias discovered in AI outputs that may have affected previous client deliverables
- Security breaches involving AI-processed sensitive data
- Systematic failures suggesting broader problems with our AI governance approach

These incidents must be reported to Managing Partners, DPO, and the Analytics Team as soon as they are discovered.

Final Reflections

AI is a powerful tool, but it's just that – a tool. At Laterite, it complements the expertise, integrity, and care that define our work. We use it thoughtfully, transparently, and only when we can stand behind the results.

This policy will continue to evolve as technology and regulations change, but our commitment to responsible, ethical research remains constant.

laterite

DATA | RESEARCH | ANALYTICS

From data to policy

www.laterite.com