

Responsible AI Policy

DAIVID Ltd | 8 October 2026

Our commitment

DAIVID is committed to developing and using artificial intelligence responsibly. We aim to provide useful creative intelligence while protecting people's rights, managing risks and being clear about the capabilities and limitations of our services.

This policy applies to AI developed or used by DAIVID, including predictive models, generative AI, third-party AI services and AI-assisted workflows. It covers our directors, employees, contractors and consultants and informs our expectations of suppliers and partners.

Purpose and appropriate use

Our creative intelligence services help organisations assess advertising and content, predict likely audience responses and inform creative and media decisions. Outputs such as attention, emotion, recall and intent predictions are estimates that should be interpreted in context. They do not guarantee an individual's response or a particular commercial outcome.

We define intended uses and assess risks before introducing an AI system or a material change. We consider the people affected, the data involved, the consequences of errors and applicable legal and contractual requirements. Our services are not designed to make decisions about an individual's employment, credit, healthcare or eligibility for essential services.

We do not permit use of our services for unlawful discrimination, deceptive practices or harmful exploitation of vulnerable people. Potentially harmful or inappropriate uses should be raised for review.

Validation reliability and monitoring

We evaluate predictive models against appropriate human response data and use testing that separates model development from evaluation, including suitable hold-out or cross-validation methods. We consider whether the sample, metric and test conditions support the intended claim.

We assess performance in relevant contexts, including markets, languages, creative formats and audiences where appropriate data is available. We monitor material changes in performance and investigate unexpected results. Limitations in coverage or sample size should be reflected in how outputs are presented and used.

For AI-generated recommendations and summaries, we assess whether the output is supported by the underlying data and identify risks such as fabricated facts or misleading explanations. Material issues may require correction, further testing or restriction of the affected feature.

Human oversight and accountability

People remain accountable for the design, deployment and use of our AI. Oversight is proportionate to the risk and purpose of the activity. Routine predictions may be generated automatically; material changes and higher-risk uses require appropriate review by authorised personnel.

Clients should review recommendations alongside their objectives, brand requirements and other relevant evidence before acting. Where AI-enabled workflows can take actions, we define their permissions and limits and require appropriate authorisation for material external actions. We seek to make it possible to stop or override an automated action where needed.

Fairness and inclusion

We consider potential bias in data, research methods, model outputs and recommendations. Where relevant and lawful, we assess differences in performance across audiences and contexts and take proportionate steps to address material issues.

We recognise that culture, language, representation and data coverage can affect predictions. We seek to avoid unfair exclusion and stereotypes and communicate limitations that could affect interpretation. We do not assume that strong overall performance establishes equivalent performance for every audience.

Privacy data rights and confidentiality

We use data for lawful, defined purposes and apply appropriate controls throughout the AI lifecycle. We consider the source of data, permissions, intellectual property rights, confidentiality, retention and applicable data protection requirements. We minimise personal data where practicable and use anonymisation or other safeguards where appropriate.

Research involving participants, including facial coding or eye tracking where used, requires suitable privacy information, permissions and safeguards. We assess whether particular processing involves sensitive personal data or additional legal requirements based on its purpose and operation.

Client materials are used only for purposes authorised by the agreed terms and applicable law. Any use for model training or improvement must fall within those permissions and requirements. Personal data or confidential material must not be entered into an unapproved AI tool. For approved providers, we assess their terms and controls, including retention, training use, access and international transfers.

Security and third party AI

We apply appropriate security controls to AI systems, data and access. We consider risks such as unauthorised disclosure, malicious inputs, prompt injection and misuse of connected tools. Controls are proportionate to the system and may include access restrictions, input handling, permission limits, testing and monitoring.

We assess third-party AI providers before use and review material changes to their services or terms. Integrating an external model does not remove our responsibility to assess its suitability and manage risks within DAVID's services.

Transparency and explanation

We explain the role of AI in our services and provide information about intended use, relevant metrics and material limitations. We distinguish predicted results, observed research findings and AI-generated recommendations so that users can interpret them appropriately.

We aim to provide understandable explanations of outputs and their basis, while protecting personal data, confidential information and intellectual property. We describe validation evidence accurately and avoid presenting correlation as proof of causation or a benchmark result as a guarantee of future performance.

Concerns incidents and review

Clients, research participants and other affected people can raise a concern or request clarification through their DAIVID contact or the contact details on our website. Team members should raise concerns with their manager or a senior leader, using another senior leader if the concern involves the usual contact.

We assess concerns fairly, seek relevant evidence and provide an appropriate response. Where an issue may affect safety, privacy, security or the reliability of outputs, we investigate and take proportionate action, which may include correcting an output, notifying affected parties where appropriate or required, or pausing an affected feature.

The CEO oversees this policy. The CTO leads technical implementation and security, with the data science lead responsible for model evaluation and relevant performance monitoring. We maintain proportionate records of material assessments, approvals, changes and incidents and provide guidance to people using AI in their work.

We review this policy at least annually and when material changes in our technology, uses or legal requirements require it. We use testing, monitoring and feedback to improve our approach. We assess applicable AI obligations for each relevant activity and jurisdiction.