Wayve Ethics Policy

Why this policy exists

We believe long-term success depends on doing the right thing: lawfully, fairly, and with respect for people and the planet. This policy sets clear expectations for everyone who represents Wayve Technologies Limited and its group of companies (together, "**Wayve**").

1. Scope

This policy applies to all employees, officers, directors, contractors, agency workers, interns, and all sites of operations. Suppliers and partners are expected to meet ethical standards as part of the Supplier Code of Conduct (see **Related Policies & Linked Documents**).

2. About us and Our Values

Founded in 2017, Wayve is a leader in artificial intelligence, pioneering Embodied AI technology for the automotive industry. This advanced technology equips robotic systems, such as automated vehicles, with the ability to interact with and learn from their surroundings, enhancing the usability and safety of assisted and automated driving systems.

Wayve has adopted the following company values:

- Big problems ignite us.
- Aim high. Stay humble.
- Back each other to deliver impact.

We believe that our values are consistent with acting in an ethical manner. We act with integrity by being honest, keeping promises, and owning our mistakes. We treat people with respect and dignity, and aim to build teams that reflect the diversity of the places where we operate. We embrace new perspectives, backgrounds, and experiences to develop products that cater to the diverse needs of the world. We aim to create a culture of inclusion and belonging where everyone feels valued and empowered to succeed. We compete fairly and lawfully, and we are transparent and accountable for our decisions and actions.

3. Legal & Regulatory Compliance

We comply with all applicable laws and regulations wherever we operate, including anti-bribery and anti-corruption, data protection and privacy, competition and antitrust, trade controls and sanctions, health, safety and environmental requirements, and labour and employment laws.

4. Professional Conduct

We treat colleagues, customers, suppliers, and the public with courtesy and professionalism. We communicate responsibly across email, chat, and social media and we do not disclose confidential information or speak on behalf of Wayve unless authorised. We use company assets and systems for legitimate business purposes and only for reasonable personal use that does not interfere with work or breach this policy.

5. Conflicts of Interest

We avoid situations where personal interests conflict, or appear to conflict, with the company's interests. As part of onboarding, we ask employees to disclose any outside employment, advisory roles or board seats, any financial interests in suppliers, customers or competitors (other than de-minimis holdings in publicly traded companies), any close personal relationships that overlap with business decisions such as hiring, performance reviews or procurement, and maintain a register for continuous compliance.

6. Gifts, Hospitality & Expenses

We do not offer, give, request, or accept anything of value to improperly influence a decision. As an employee, we obtain pre-approval for gifts or hospitality above our required thresholds, or involving public officials. We do not provide or accept cash or cash equivalents such as gift cards. We record all expenses accurately and submit receipts, and do not submit false or misleading claims. Our gifts and hospitality policy details this further.

7. Anti-Bribery & Anti-Corruption (ABAC)

We prohibit bribes, kickbacks, facilitation payments, and any improper advantage, whether offered directly or through third parties. We conduct proportionate due diligence on intermediaries, agents, and high-risk suppliers.

8. Money laundering and fraud

We do not engage in or facilitate money laundering or terrorist financing. We maintain a zero tolerance approach to financial crimes and fraud. All employees and suppliers are expected to act honestly and transparently in financial dealings. Any concerns or suspicions regarding fraudulent or illegal financial activity should be reported immediately to the Finance team. Misuse of company funds may be subject to disciplinary proceedings.

9. Prohibited Dealings with Criminal Organisations & Unlawful Groups

We will not engage in or facilitate any relationship, transaction, or activity, whether directly or indirectly, with criminal organisations, organised crime syndicates, extremist or violent groups, or front companies acting on their behalf, as defined by applicable law. We prohibit so-called protection payments and any other coerced or unjust demands. We strengthen counterparty due diligence in higher-risk geographies and sectors, and any suspected link must be escalated to Legal.

10. Fair Competition

We compete vigorously but lawfully. We do not discuss or agree with competitors on prices, bids, market allocation, production levels, or boycotts, and we exchange only market information that is necessary, aggregated, and lawful.

11. Information Handling: Confidentiality, IP, & Records

We protect confidential information by applying security good practice to our systems and services, requiring the same of our supply chain, and sharing only on a need-to-know basis. We always ensure appropriate confidentiality agreements are in place before sharing or receiving confidential or sensitive information. We respect third-party intellectual property and licences and we do not use unapproved datasets, software, or models. We keep accurate records and follow retention schedules and legal holds.

12. Data Protection & Security

We handle personal data lawfully, fairly, and transparently and we process only what is necessary for a defined purpose. We follow security policies for strong authentication, encryption, device hardening, and incident reporting. Any data incident must be reported immediately through the designated channel.

13. Suppliers

We select suppliers through fair and transparent processes and we manage third-party risks through proportionate due diligence and contract controls. We expect suppliers to uphold the standards as set out in a Supplier Code of Conduct; where appropriate, we seek contractual commitments or other suitable assurances.

14. Whistleblowing

Employees and other stakeholders have the ability to address concerns, including criminal offences, health and safety risks, actual or risk of damage to the environment or legal violations. Concerns may be raised through the means outlined in the Whistleblowing Policy. Reports will be treated confidentially, and where requested, anonymously. Retaliation against anyone who raises a good faith concern or participates in an investigation is strictly prohibited and will result in disciplinary action.

15. Governance & Policy Management

- **Roles & responsibilities:**
  - **Chief Financial Officer:** accountable to the board for the effectiveness of the policy.
  - **Data Protection Officer (DPO):** privacy governance and incident oversight.
  - **Managers:** model behaviour, ensure team training completion, and manage conflicts/gifts registers.
- **Policy duration:** reviewed at least annually; material changes require approval by the Chief Financial Officer
- **Registers:** Finance team maintain registers on gifts and hospitality and travel and expenses. .

16. Questions & Contacts

For questions on the Ethics Policy please discuss with the Finance team in the first instance.

17. Related Policies & Linked Documents

This Ethics Policy should be read alongside the **Human Rights Policy**, the **Environmental Policy**, the **Supplier Code of Conduct**, and the **Whistleblowing Policy**.

18. Ethics Policy Targets

Our goal is that in FY26 and FY27, 95% of our employees have completed cyber security training.

Version	Effective Date	Next Review	Summary
1.0	14/11/2025	Nov 2026	First Version