PUIG

Policy on the responsible use of artificial intelligence systems

Purposes

The **Puig**[1] Ethical Code establishes the values and commitments that it assumes internally and externally as an organization. Within the framework of these commitments, and aware of the relevance and impact that the development and/or use of artificial intelligence tools and/or systems (hereinafter, "AI Systems")[2] may entail, Puig promotes responsible use, based on ethics and sustainable development.

This Policy on the Responsible Use of Artificial Intelligence Systems (hereinafter, "**Policy**") reflects **Puig**'s commitment to fostering innovation through the ethical, responsible, transparent, and legally compliant use of AI Systems, ensuring safety, reliability, and the protection of fundamental rights. It outlines the core principles and minimum standards guiding the development, deployment, implementation and use of AI Systems as part of **Puig**'s digital transformation strategy.

Scope

This Policy has been approved by the CEO of Puig Brands, S.A. and applies to all **Puig** employees (regardless of their seniority, role, or location), companies and businesses, and promotes compliance among external stakeholders (suppliers, clients, third party companies and professionals, etc.) to the extent that they develop, license, deploy and/or use AI Systems for **Puig**.

The Policy applies alongside other compulsory internal regulations such as the Information Security Policy, Privacy Policy and other standards and guidelines regarding the use of AI Systems within **Puig**.

Under no circumstances shall the application of this Policy result in non-compliance with current legal provisions in force in the markets in which **Puig** operates. These provisions shall prevail over this Policy in all circumstances.

The various local **Puig** divisions and business units can implement this Policy via other local or division-specific policies, committees and procedures that comply with the terms, principles and conduct contained in this Policy.

It is the responsibility of the company's highest governing body, **Puig** managers, and all employees in general, to be aware of, comply with, and ensure compliance with the contents of this Policy. The **Puig** AI General Committee will supervise the Policy's implementation and modification, and will ensure that it is suitably executed.

[1] "**Puig**" and/or the company, refer to the company Puig Brands, S.A., and its subsidiaries and any other legal entity that may be established in the future, over which Puig Brands, S.A. holds or may hold direct or indirect control, in accordance with article 42 of the Spanish Commercial Code.

[2] "AI system" For the purposes of this Policy, an AI System means a machine-based system that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments. Different AI systems vary in their levels of autonomy and adaptiveness after deployment.

Principles and commitments

Principles

This Policy is guided by a set of core principles, aligned with the **Puig** Ethical Code and applicable regulations. These core principles are outlined below:

- **Respect for people, sustainability, and well-being**: AI Systems will be developed and/or used to serve people and the planet, upholding human rights and promoting inclusive growth, sustainable development and overall well-being. **Puig** is committed to aligning AI practices with its broader ESG goals to help build a more sustainable and responsible future.

- **Diversity, non-discrimination, and fairness:** AI Systems will be developed, implemented, deployed and/or used in ways that promote fair treatment and avoid discrimination based on race, religion, gender, sexual orientation, age, disability, or other personal or cultural traits. Human oversight will be promoted and required to prevent bias and unfair outcomes.

- **Transparency.** AI Systems will be developed, implemented, deployed and/or used with clarity, openness and fairness, in a way that allows for adequate traceability and transparency, ensuring that users and/or people affected by the use of such AI systems are aware that they are communicating or interacting with an AI System. To this end, **Puig** will strive to explain to affected individuals about the capabilities and limitations of these systems, how they work, their purpose, security, and the principles that govern them, making such technologies understandable to all stakeholders as well as the rights that protect them.

- **Integrity and privacy:** AI Systems will be developed, implemented, deployed and/or used in accordance with privacy and data protection regulations. In any case, the collection, processing, and storage of all data (including but not limited to personal data) will be carried out respecting the principles of quality and integrity of the data, as well as any other principles established in the Privacy Policy and the data privacy regulations and standards.

- **Intellectual property and image rights:** AI Systems will be developed, implemented, deployed, and/or used in accordance with the intellectual property and image rights regulations. **Puig** strives to respect third parties' intellectual property and image rights and is committed to avoiding the use of any AI Systems in ways that, knowingly, could infringe third parties' rights.

- **Robustness and security:** AI Systems must operate reliably and securely throughout their lifecycle, with ongoing risk assessment and mitigation.

- **Accountability:** Anyone involved in developing, deploying, or using AI Systems at **Puig**, whether internal or external, must ensure that these systems function responsibly and in line with this Policy.

Commitments

Regarding the principles underpinning this Policy, **Puig** adopts the following commitments:

- All AI Systems developed and/or used must comply with relevant laws, regulations, and ethical standards.

- All AI Systems must be approved and signed off for use by the AI Demand Management Committee before being deployed for live use within **Puig**.

- All AI Systems must align with **Puig** security standards and policies to protect **Puig** confidential and restricted information and, when AI Systems collect and process personal data, these will comply with applicable data privacy regulations and policies.

- The use and development of AI System will be subject to tests and validations to ensure that the resulting data is free from biases, inaccuracies, unfair prejudice or discriminatory tendencies. Any AI System found to be promoting such behaviors will be halted and immediately remediated.

- Any deployment of an AI System must prioritize and ensure accessibility for all personnel, regardless of ability. Considerations for universal design and inclusivity shall be integral to the development, deployment and use of all AI Systems within **Puig**.

- Ensure the ethical development of all AI systems whether developed in-house or procured on an external basis from third parties, and irrespective of whether use is for internal or external purposes.

- Development, deployment, implementation and/or use of AI Systems at **Puig** must be overseen by **Puig**'s personnel at all times[3], irrespective of its associated risk level. output data from an AI System must always be checked by **Puig** personnel before being further used or otherwise distributed within the business. This is mandatory for all AI Systems.

AI - general considerations

Prohibited AI systems

Certain types of AI System may be prohibited by applicable regulations and are, therefore, prohibited from being developed, deployed, implemented or used in any capacity at **Puig**. These AI Systems include, by way of illustration:

- Any AI System which deploys subliminal, manipulative or deceptive components or techniques which individuals cannot perceive and/or which exploit other vulnerabilities (e.g. age, disability, or social or economic situation) to materially distort their behavior in a manner that causes or is likely to cause harm.[4]

- Any AI System used for social scoring (classifying people based on their social behavior, socio-economic status or personal characteristics) of individuals, including evaluating the trustworthiness of individuals based on social behaviour.[5]

- Any real-time remote biometric identification of individuals in publicly accessible spaces except for certain purposes related to law enforcement.[6]

- Any AI System for detecting or interpreting emotions in contexts such as the workplace or educational settings where this may affect decisions about individuals.

[3] These steps are essential to maintain a continuous review and assessment of output data, automated decision making, and actions proposed or taken by the AI System. Puig must be able to demonstrate that it is actively taking steps to reduce potential biases and discrimination that might arise from AI decision making processes.

[4] For example, use of such technology to influence individuals to make purchasing decisions they cannot afford or to engage in games of chance.

[5] For example, an AI System deployed in a credit vetting process where social scoring informs the outcome of the assessment.

[6] For example, identification and surveillance technology used by the police.

Other types of AI systems

Any type of AI System not identified above as being Prohibited will also be assessed[7] and evaluated in accordance with the AI Demand Management Process ("**Approval Process**") outlined at the approval section below.

<u>Limited internal use exception</u>: As a general rule, all AI Systems must be approved by the AI Demand Management Committee before use. However, employees are permitted to use unapproved AI Systems on a limited basis for internal purposes only, provided all the following conditions are met:

- **No confidential data:** No confidential **Puig** or third parties' works, information or personal data may be input into any unapproved AI System. Employees must never disclose restricted or sensitive content in prompts or queries.

- **Internal use only:** AI System's output may be used solely for internal inspiration or draft work (e.g. brainstorming, initial drafts), and not for any final materials. AI-generated content must not be published, presented to clients, or otherwise utilized externally without proper approval.

- **Review and accountability:** Employees must carefully review any AI-generated result for accuracy, legality, and compliance with **Puig** policies before using it. The employee assumes responsibility for the content and will be held accountable for misuse of the AI System.

- **External use requires approval:** If an employee wishes to use AI-generated material in any external context (e.g. in a product design, marketing campaign, or published content), they must use an AI System approved by the AI Demand Management Committee and follow the internal IP Legal validation process and/or guidelines prior to external use (just as with any non-AI-generated creative content) namely for products and campaign key assets, as well as for any other assets created on the basis of a specific inspiration source. This might entail sharing the AI prompt, inputs and other relevant details related to the creative material with the IP Legal team during the review.

[7] These AI Systems are likely to be subject to applicable transparency requirements including measures such as notifying individuals that they are interacting with an AI System and/or that content has been generated by an AI System. The necessary transparency requirements which will apply to AI Systems of this type will need to be assessed on a case by case basis depending on each anticipated use case for the AI System concerned.

Approval of AI systems

All **Puig** personnel must seek and obtain approval from the AI Demand Management Committee before any development, deployment, implementation or use of an AI System within **Puig**. The project owner for each AI System or any new use case, must adhere to the AI Demand Management Process before proceeding with the development, deployment and/or use of any AI System within **Puig**.

- The AI Demand Management Committee, together with the relevant business unit, will conduct enhanced due diligence and analysis (including ethical use considerations, where relevant) into potential risks and benefits of the AI System and the intended use (use case). Third party AI Systems will be subject to stringent vendor assessments to ensure such AI Systems meet **Puig** standards and applicable regulatory and security requirements.

- AI Systems may not be used under any circumstances unless prior explicit written authorization has been granted by the AI Demand Management Committee, and only within the scope of such authorization. Silence, lack of response, or inaction shall not be interpreted as implied or tacit approval.

- Approval from the AI Demand Management Committee, shall only be granted after a thorough assessment ensuring that the use case for the AI System aligns with **Puig** governance standards on the use of AI Systems and applicable regulatory requirements and this Policy (the "**Initial Approval**").

- Any significant changes to the scope of an AI System that is the subject of Initial Approval, including changes to the use, purpose, functionality or scope of deployment of the AI System must be further approved through the **Approval Process** (where relevant).

- Product and/or project owners/managers (as applicable) will be responsible for conducting regular self-assessments on the use of approved AI Systems, with periodic reporting to the AI Demand Management Committee, to ensure ongoing adherence to **Puig** AI governance standards.

- The notification of any security incident affecting the use of AI tools must be addressed in accordance with the Corporate Incident Management Policy defined at **Puig**. Each tool must have a designated business owner as well as a resolution contact); this refers to the technical resolution team (internal or external) associated with the tool, acting as the point of contact. Any data breaches or security incidents must be communicated to incidents.security@puig.com.

Obligations of **Puig** employees

As a **Puig** employee, you must always act in a responsible manner and in accordance with the **Puig** Ethical Code and any other **Puig** Policies. By accessing or using AI Systems, you agree to the following basic conditions:

- Comply with this Policy and any other related regulations or specific guidelines regarding the development, deployment and/or use of AI Systems.

- Never use any AI System that has not been expressly approved by the AI Demand Management Committee, except as allowed under the limited internal use exception outlined in this Policy (i.e., use of unapproved AI Systems for strict internal purposes, without confidential data and under specified conditions).

- Ensure that any access or use of AI Systems should be granted through licenses contracted directly by **Puig**, and that they will be used by those users to whom **Puig** has granted access for the performance of their duties. You should never share your corporate credentials.

- If you are using any AI System under a license contracted directly by **Puig**, please note that such use is strictly limited to individual access. User accounts and credentials are personal and non-transferable, and must not be shared with any other person, whether inside or outside the organization. Each user is fully responsible for the activity conducted under their assigned account. All employees are expected to use licensed AI tools in accordance with the applicable terms of service, internal security protocols, and this Policy.

- Cooperate in implementing any measures required and provide information or documentation when requested to demonstrate compliance with this Policy and relevant regulations.

- Never use any AI System in a manner that results in, or perpetuates, bias, discrimination or any form of unethical or unlawful behavior.

- Never use the AI Systems for mass analysis of personal data (e.g., consumer and/or employee data) or for individual automated decision-making (including profiling) for example any form of personal data processing that evaluates personal aspects, such as analyzing or predicting aspects related to work performance, economic situation, health, personal preferences or interests, reliability, or behavior. If you are unsure as to whether a potential use of an AI System is compliant in this regard, you should contact the AI Demand Management Committee.

- Never include in AI Systems, **Puig**’s original works or search parameters, queries and/or prompts that may generate results that infringe the rights of third parties or be considered specifically intended to infringe third parties rights (for example, but not limited to, terms such as, "inspired by," "similar to, “imitating”, "copying," or "in the style of").

- If an employee wishes to use AI-generated material in any external context (e.g. in a product design, marketing campaign, or published content), they must use an AI System approved by the AI Demand Management Committee and follow the internal IP Legal validation process and/or guidelines prior to external use (just as with any non-AI-generated creative content), namely for products and campaign´s key assets, as well as for any other assets created on the basis of a specific inspiration source. This might entail sharing the AI prompt, inputs and other relevant details related to the creative material with the IP Legal team during the review.

- Understand and accept that content generated by AI Systems may not always be accurate and, therefore, Employees are responsible for reviewing and validating any information or result obtained through an AI System before using it.

- Attend training and awareness-raising initiatives relating to this Policy, the use of AI Systems or AI in general.

- Inform the AI Demand Management Committee if you become aware that the implementation of this Policy does not comply with applicable local laws or regulatory requirements in the jurisdictions where **Puig** operates. This ensures that any necessary adaptations or corrective actions are addressed in a timely and coordinated manner.

- Contact the AI General Committee via email aipolicy@puig.com to address issues related to this Policy, the development and/or use of AI systems and any other means, mechanism, and/or platforms enabled for this purpose. Additionally, as part of the **Puig** "Speak Up" culture, if potential non-compliance with this Policy is suspected or identified, **Puig** encourages reporting it through the **Puig** Reporting Channel available at the following link https://puigreportingchannel.ethicspoint.com.

- Report any breach of this Policy via the points of contact mentioned above.

Governing bodies and persons responsible for this Policy

The following bodies and persons are responsible for this Policy:

- The CEO appoints the **AI General Committee** as the body responsible for establishing the foundational framework for effective and ethical AI governance, ensuring alignment with **Puig**'s strategic objectives. This AI General Committee is responsible for defining and overseeing key aspects such as AI policies, ethical principles, responsible usage guidelines, and high-level project tracking, facilitating cross-functional collaboration and comprehensive oversight. It is also entrusted with the following functions:

  - The AI General Committee will be responsible for defining Puig's AI strategy and will determine the different use cases, projects and initiatives related to AI as the business needs.

  - The AI Committee will appoint and oversee the AI Demand Management Committee in carrying out its duties of approving, implementing and monitoring Puig's AI projects using AI Systems. This oversight is crucial to ensure that all AI related initiatives comply with the applicable regulations and standards.

  - Review this Policy regularly to reflect changes resulting from emerging technologies and technological advance, the evolving landscape of AI ethics and best practice, legislation and regulatory developments and organizational change. Such reviews should include new or revised processes, controls, or changes in the risk profile of the business to ensure that it remains suitable.

    - Monitor the application of and compliance with applicable regulations and this Policy, the procedures that derive from them, their associated processes and controls (including the corresponding authorizations, approvals, audits, monitorizations), and the allocation of responsibilities.

    - Promote training and awareness within Puig on use of AI Systems, ensuring that all employees understand this Policy and the standards that Puig expects employees to adhere to with regards to AI Systems and associated risks.

    - Report any circumstances or information that may have an impact on compliance with this Policy and the obligations arising from applicable regulations to Puig's CEO, or to whomever the CEO may designate. Any matter or conflict that cannot be resolved within the AI General Committee or the AI Demand Management Committee shall likewise be escalated to the CEO or the CEO's designee for final decision.

- **The AI Demand Management Committee** has been assigned by the AI General Committee to oversee and manage AI initiatives across **Puig**. This includes assessing AI Demand through business cases and technical and legal feasibility, monitoring delivery and initiatives performance through KPIs, to make informed decisions on projects feasibility, continuation, adjustments, or resource reallocation. Its primary functions include:

    - Validating, in coordination with the relevant areas, the deployment and implementation of the different use cases, projects, initiatives related to AI and the relevant AI Systems.

    - Facilitating cross-departmental communication and collaboration by bringing together experts from different areas to ensure that AI initiatives are aligned with **Puig**'s AI strategy and objectives, fostering a more cohesive and integrated approach to AI deployment.

    - The AI Demand Management Committee should also be responsible in collaboration with the relevant areas, for conducting risk assessments and implementing mitigation strategies. This involves identifying potential risks associated with AI Systems, such as ethical concerns, data privacy issues, and security vulnerabilities, and taking appropriate measures to address these risks proactively.

- Promoting transparency and accountability in AI usage. This includes ensuring that AI Systems are explainable and that their decision-making processes can be understood and scrutinized by relevant stakeholders. It is also important to establish clear lines of accountability for AI-related decisions and actions.
- Coordinating training and awareness-raising AI initiatives for employees taking part in the development, deployment and/or use of AI Systems with the relevant areas.
- Reporting any circumstances or information that may have an impact on compliance with this Policy and the duties arising from regulations to the AI General Committee, the Audit Committee, the Executive Committees of the business divisions and/or the corporate functions.

Approval, publication, and review

This Policy has been approved by the CEO of Puig Brands, S.A. on 10 December 2025, and came into force at the same time. In addition, it has been published and is available on the Ethics Home platform https://puig.sharepoint.com/sites/ETHICSHOME, **Puig** website, and will be sent to **Puig** employees and other interest groups where applicable.

The AI General Committee, in coordination with the relevant areas, will be responsible for publishing, reviewing, updating and improving this Policy where necessary. This Policy supersedes and replaces any previous policy.

In the event of non-compliance with this Policy, **Puig** will take legal (including disciplinary) or contractual measures, as appropriate to the nature of the non-compliance.